ผลและการวิเคราะห์ข้อมูลการดาวน์โหลดมัลแวร์/บ็อทในญี่ปุ่น

RESULTS AND ANALYSIS OF MALWARE/BOT DOWNLOAD IN JAPAN

วัชรวิชญ์ สุวรรณชัยศักดิ์
WATCHARAWIT SUWANCHAISAK

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
พ.ศ. 2558
KMITL-2015-EN-M-070-017

ผลและการวิเคราะห์ข้อมูลการดาวน์โหลดมัลแวร์/บ็อทในญี่ปุ่น

RESULTS AND ANALYSIS OF MALWARE/BOT DOWNLOAD IN JAPAN

วัชรวิชญ์ สุวรรณชัยศักดิ์
WATCHARAWIT SUWANCHAISAK

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต
สาขา วิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
พ.ศ. 2558
KMITL-2015-EN-M-070-017

RESULTS AND ANALYSIS OF MALWARE/BOT DOWNLOAD IN JAPAN

WATCHARAWIT SUWANCHAISAK

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENT FOR THE DEGREE OF
MASTER OF ENGINEERING IN COMPUTER ENGINEERING
FACULTY OF ENGINEERING
KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG
2015
KMITL-2015-EN-M-070-017

คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ใบรับรองวิทยานิพนธ์

หัวข้อวิทยานิพนธ์ ผลและการวิเคราะห์ข้อมูลการดาวน์โหลดมัลแวร์/บ็อทในญี่ปุ่น
Thesis Title Results and Analysis of Malware/Bot Download in Japan
นักศึกษา นายวัชรวิชญ์ สุวรรณชัยศักดิ์
รหัสประจำตัว 53611104
ปริญญา วิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชา วิศวกรรมคอมพิวเตอร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์ ผศ.ดร.สุรินทร์ กิตติธรกุล
หมายเลขวิทยานิพนธ์ KMITL-2015-EN-M-070-017

คณะกรรมการสอบวิทยานิพนธ์		ลายมือชื่อ
ผศ.ดร.ศักดิ์ชัย	ทิพย์จักษุรัตน์	
ดร.วรวัฒน์	ลิ้มโภคา	
ผศ.ดร.ภุชงค์	อุทโยภาศ	
รศ.ดร.บุญวัฒน์	อัตชู	
ผศ.ดร.สุรินทร์	กิตติธรกุล	

วัน / เดือน/ ปี ที่สอบ วันจันทร์ที่ 16 กุมภาพันธ์ พ.ศ. 2558 เวลา 10.00-12.00 น.
สถานที่สอบ ณ อาคาร ECC ห้อง ECC-810

คณะวิศวกรรมศาสตร์ รับรองแล้ว

(รองศาสตราจารย์ ดร. คมสัน มาลีสี)

คณบดี คณะวิศวกรรมศาสตร์

วันที่ 16 กุมภาพันธ์ พ.ศ. 2558

หัวข้อวิทยานิพนธ์	ผลและการวิเคราะห์ข้อมูลการดาวน์โหลดมัลแวร์/บ็อทในญี่ปุ่น
นักศึกษา	นายวัชรวิชญ์ สุวรรณชัยศักดิ์
รหัสนักศึกษา	53611104
ปริญญา	วิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชา	วิศวกรรมคอมพิวเตอร์
พ.ศ.	2558
อาจารย์ที่ปรึกษาวิทยานิพนธ์	ผศ.ดร.สุรินทร์ กิตติธรกุล

บทคัดย่อ

ปัจจุบัน มัลแวร์ได้กระจายไปทั่วระบบอินเตอร์เน็ตโดยใช้บ็อทเน็ตเป็นตัวนำในการดาวน์โหลด ซึ่งวิทยานิพนธ์ฉบับนี้จะนำเสนอพฤติกรรมการดาวน์โหลดของ Top-10 มัลแวร์ จากล็อกข้อมูล CCC (Cyber Clean Center) ปี ค.ศ.2010 และ 2011 ซึ่งประกอบด้วยล็อกข้อมูลของการดาวน์โหลดจากเครื่องฮันนีพอต (Honeypots) ต่างๆ ในประเทศญี่ปุ่น เพื่อใช้ในการตรวจสอบพฤติกรรมต่างๆ ของมัลแวร์ ผู้วิจัยได้พิจารณาการดาวน์โหลดมัลแวร์แบบรายชั่วโมง และรายวัน รวมถึงข้อมูลของหมายเลขไอพี แอดเดรสต้นทางที่มัลแวร์ใช้งานร่วมกัน

Thesis Title	Results and Analysis of Malware/Bot download in Japan
Student	Mr. Watcharawit Suwanchaisak
Student ID	53611104
Degree	Master of Engineering
Program	Computer Engineering
Year	2015
Thesis Advisor	Asst.Prof.Dr. Surin Kittitornkun

ABSTRACT

Nowadays, malware can be spread over the Internet using botnets to download. This thesis presents temporal download behavior of Top-10 malware base on 2010 and 2011 CCC (Cyber Clean Center) datasets that consist of download logs of several independent honeypots in Japan to observe malware traffic and its activities. Our results show sequences and similar patterns of malware downloads in terms of number of downloads per hour and per day including common source IP addresses.

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงได้ดี เพราะด้วยความช่วยเหลืออย่างดียิ่งจากอาจารย์ที่ปรึกษาวิทยานิพนธ์ ผศ.ดร.สุรินทร์ กิตติธรกุล ที่ได้อบรมสั่งสอนวิชาความรู้ให้แก่ข้าพเจ้า คอยให้คำปรึกษา คำแนะนำ และชี้แนะแนวทางในการดำเนินการวิจัย รวมถึงกำลังใจที่ท่านได้มอบให้ตลอดมา เป็นสิ่งที่ข้าพเจ้าซาบซึ้งและขอกราบขอบพระคุณท่านมา ณ ที่นี้

ขอขอบคุณคณาจารย์ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบังทุกๆ ท่านที่ได้ประสิทธิ์ประสาทวิชาให้กับข้าพเจ้า

ขอขอบคุณพี่ๆ เพื่อนๆ และน้องๆ ในภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบังทุกคนที่ให้คำแนะนำต่าง ๆ และคอยให้กำลังใจเสมอมา

สุดท้ายนี้ข้าพเจ้าขอกราบขอบพระคุณบิดา มารดา ครอบครัวและภรรยาที่รักยิ่งของข้าพเจ้าที่คอยเป็นกำลังใจ และให้การสนับสนุนในทุกๆ เรื่อง รวมถึงการอบรมสั่งสอน และให้คำแนะนำแก่ข้าพเจ้า

คุณค่าและประโยชน์อันพึงมีจากวิทยานิพนธ์ฉบับนี้ ข้าพเจ้าขอมอบแต่ผู้มีพระคุณทุก ๆ ท่านไว้ ณ โอกาสนี้

วัชรวิชญ์ สุวรรณชัยศักดิ์

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

สารบัญรูป

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในปัจจุบันการใช้งานผ่านระบบอินเทอร์เน็ตนั้นได้มีโปรแกรมประเภทไม่หวังดี เพิ่มมากขึ้นเป็นจำนวนมาก ซึ่งผู้ใช้งานทั่วไปอาจจะได้รับข้อมูลข่าวสาร และโปรแกรมต่างๆ โดยไม่รู้ตัว และโปรแกรมเหล่านี้ได้เข้ามาฝังตัวในเครื่องคอมพิวเตอร์ของผู้ใช้งาน แล้วอาจทำให้เกิดอาการผิดปกติของเครื่องคอมพิวเตอร์ระหว่างการใช้งานอินเทอร์เน็ต เช่น การใช้งานที่ช้าลง มีการแสดงหน้าต่างโฆษณาสินค้าขึ้นตลอดเวลา พิมพ์ภาษาไทยบนระบบ Browser ไม่ได้ จนถึงเครื่องคอมพิวเตอร์ไม่สามารถใช้งานได้และต้องเปิด-ปิด เครื่องใหม่ เป็นต้น ซึ่งอาการเหล่านี้อาจเกิดจากโปรแกรมประเภทมัลแวร์ (Malware) โดยทำงานในลักษณะที่เป็นไวรัส ทั้งประเภทเวิร์ม (Worm) หรือหนอนอินเทอร์เน็ต และพวกม้าโทรจัน (Trojan Horse) การแอบดักจับข้อมูล (Spyware) และการดักจับคีย์บอร์ด (Key Logger) บนเครื่องคอมพิวเตอร์ของผู้ใช้งาน ตลอดจนโปรแกรมประเภทขโมยข้อมูล (Cookie) และการฝัง Malicious Mobile Code (MMC) ผ่านทางช่องโหว่ของโปรแกรม Internet Explorer (IE Vulnerability) ที่เกิดขึ้น โดยโปรแกรมจะทำการควบคุมการทำงานโปรแกรม Internet Explorer ให้เป็นไปตามความต้องการของผู้ที่ไม่หวังดี เช่น การแสดงโฆษณาในลักษณะของการ Pop-Up หน้าต่างโฆษณาออกมาเป็นระยะ เราเรียกโปรแกรมประเภทนี้ว่า แอ็ดแวร์ (Adware) ซึ่งภัยเหล่านี้ในปัจจุบันได้เพิ่มขึ้นอย่างรวดเร็ว ซึ่งอาจจะเกิดผลกระทบแก่ผู้ใช้งานได้ ถ้ารับโปรแกรมเหล่านี้เข้ามาในเครื่องคอมพิวเตอร์

มัลแวร์ (Malware)

มัลแวร์ (Malware) ย่อมาจากคำว่า Malicious Software ซึ่งหมายถึงโปรแกรมประสงค์ร้ายต่างๆ โดยทำงานในลักษณะที่เป็นการโจมตีระบบ การทำให้ระบบเสียหาย รวมไปถึงการโจรกรรมข้อมูล มัลแวร์ แบ่งออกได้หลากหลายประเภท อาทิเช่น ไวรัส (Virus) เวิร์ม (Worm) หรือหนอนอินเทอร์เน็ต ม้าโทรจัน (Trojan Horse) การแอบดักจับข้อมูล (Spyware) การดักจับคีย์บอร์ด (Key Logger) บนเครื่องคอมพิวเตอร์ของผู้ใช้งาน ตลอดจนโปรแกรมประเภทขโมยข้อมูล (Cookie) และการฝัง Malicious Mobile Code (MMC) ผ่านทางช่องโหว่ของโปรแกรม Internet Explorer (IE Vulnerability) ที่เกิดขึ้น โดยโปรแกรมจะทำการควบคุมการทำงานโปรแกรม Internet Explorer ให้เป็นไปตามความต้องการของผู้ที่ไม่หวังดี เช่น การแสดงโฆษณาในลักษณะของการ Pop-Up หน้าต่างโฆษณาออกมาเป็นระยะ เราเรียกโปรแกรมประเภทนี้ว่า แอ็ดแวร์ (Adware) ซึ่งภัยเหล่านี้ในปัจจุบันได้เพิ่มขึ้นอย่างรวดเร็ว ซึ่งอาจจะเกิดผลกระทบแก่ผู้ใช้งานได้ ถ้ารับโปรแกรมเหล่านี้เข้ามาในเครื่องคอมพิวเตอร์ และในปัจจุบันการใช้งานผ่านระบบอินเทอร์เน็ตนั้นได้มีโปรแกรมประเภทไม่หวังดี เพิ่มมากขึ้นเป็นจำนวนมาก ซึ่งผู้ใช้งานทั่วไปอาจจะได้รับข้อมูลข่าวสาร และโปรแกรมต่างๆโดยไม่รู้ตัว และโปรแกรมเหล่านี้ได้เข้ามาฝังตัวในเครื่องคอมพิวเตอร์ของผู้ใช้งานแล้วเพื่อที่ดักขโมยข้อมูล หรือแก้ไขตัวระบบการทำงานของคอมพิวเตอร์ให้เกิดอาการผิดปกติ ระหว่าง

การใช้งานคอม หรืออินเทอร์เน็ต เช่น อาการคอมทำงานช้า มีหน้าต่างโฆษณาแทรกตลอด พิมพ์ภาษาไทยบนระบบ Browser ไม่ได้ เข้าเว็บไซต์ไม่ได้ จนถึงเครื่องคอมพิวเตอร์ไม่สามารถใช้งานได้และต้องเปิด-ปิด เครื่องใหม่ เป็นต้น หรือขั้นท้ายสุดหมดทาง ก็ทำการลุยฟอร์แมต (format) แล้วลงระบบปฏิบัติการเครื่องครั้งใหม่ เพื่อให้สามารถทำงานปกติได้ อาการเหล่านี้อาจเกิดจากโปรแกรมประเภท มัลแวร์ (Malware) หรือคนส่วนใหญ่จะรู้จักกันที่เรียกว่า ไวรัสคอมพิวเตอร์นั่นเอง

ประวัติความเป็นมาของไวรัสคอมพิวเตอร์

โปรแกรมที่สามารถสำเนาตัวเองได้เกิดขึ้นเป็นครั้งแรกในปี พ.ศ. 2526 โดย ดร.เฟรดเดอริก โคเฮน นักวิจัยของมหาวิทยาลัยเพนซิลวาเนีย สหรัฐอเมริกา ได้ทำการศึกษาโปรแกรมลักษณะนี้และได้ตั้งชื่อว่า "ไวรัส" แต่ไวรัสที่แพร่ระบาดและสร้างความเสียหายให้กับเครื่องคอมพิวเตอร์ตามที่มีการบันทึกไว้ครั้งแรกเมื่อปี พ.ศ. 2529 ด้วยผลงานของไวรัสที่ชื่อ "เบรน" (Brain) ซึ่งเขียนขึ้นโดยโปรแกรมเมอร์สองพี่น้องชาวปากีสถาน ชื่อ อัมจาด (Amjad) และ เบซิท (Basit) เพื่อป้องกันการคัดลอกทำสำเนาโปรแกรมของพวกเขาโดยไม่จ่ายเงิน

ไวรัสคอมพิวเตอร์ในยุคแรกๆ จะระบาดโดยการสำเนาซอฟท์แวร์เถื่อนหรือซอฟท์แวร์ละเมิดลิขสิทธิ์ที่มีโปรแกรมไวรัสคอมพิวเตอร์ติดอยู่ ด้วยการใช้แผ่น floppy disk หรือซีดีรอม แต่ในปัจจุบันเนื่องจากการเติบโตของเครือข่ายคอมพิวเตอร์ทำให้ไวรัสยุคหลังๆ มีความสามารถในการทำสำเนาคัดลอกและแพร่กระจายตัวเองได้มากขึ้น รวมทั้งมีความรุนแรงมากกว่าเดิม ในปัจจุบันนี้พบว่ามีมากกว่า 40,000 ชนิด และยังเกิดเพิ่มขึ้นอีกอยู่ทุกๆ วัน อย่างน้อยวันละ 4-6 ตัว

ความหมายของไวรัสคอมพิวเตอร์

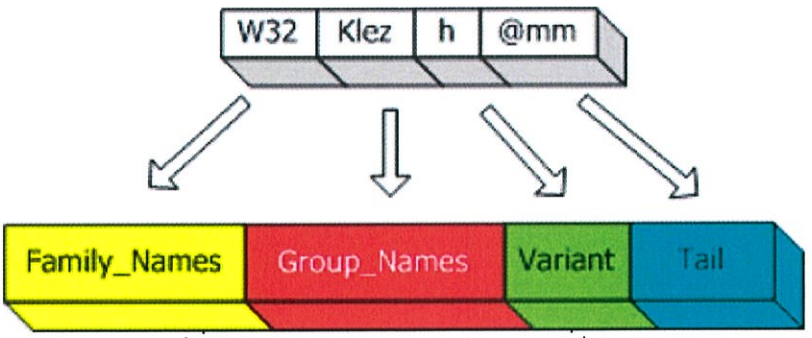
ไวรัสคือโปรแกรมชนิดหนึ่งที่ถูกเขียนขึ้นให้สามารถจัดการกับตัวมันเองโดยมีลักษณะเลียนแบบสิ่งมีชีวิต คือเจริญเติบโตเองได้ ขยายและแพร่กระจายตัวเองได้ สามารถอยู่รอดได้ด้วยการอำพรางตนเหมือนกับไวรัสที่เป็นเชื้อโรคร้ายทำลายสิ่งมีชีวิตทั้งหลายนั่นเอง

การที่คอมพิวเตอร์เครื่องใดติดไวรัส หมายความว่า ไวรัสได้เข้าไปฝังตัวอยู่ในหน่วยความจำคอมพิวเตอร์เรียบร้อยแล้ว เนื่องจากไวรัสเป็นโปรแกรมชนิดหนึ่งการที่จะเข้าไปอยู่ในหน่วยความจำได้จะต้องมีการถูกเรียกใช้งานหรือถูกกระตุ้นให้ทำงาน (ขึ้นอยู่กับประเภทของไวรัสชนิดนั้นๆ) ซึ่งปกติผู้ใช้เครื่องมักจะไม่รู้ตัวว่าได้ทำการปลุกไวรัสคอมพิวเตอร์ให้ขึ้นมาทำงานแล้ว

การทำงานของไวรัสแต่ละตัวจะขึ้นกับวัตถุประสงค์ของผู้เขียนโปรแกรมนั้นขึ้นมา เช่น ทำลายระบบปฏิบัติการ โปรแกรมใช้งานหรือข้อมูลอื่นๆ ที่อยู่ในเครื่องคอมพิวเตอร์ หรือรบกวนการทำงาน เช่น การบู๊ตระบบช้าลง เรียกใช้โปรแกรมได้ไม่สมบูรณ์ หรือเกิดอาการค้าง (แฮงค์ไม่ทราบสาเหตุ) เกิดข้อความวิ่งไปมาที่หน้าจอ หรือกรอบข้อความเตือนไม่ทราบสาเหตุ เป็นต้น

เคยสงสัยกันบ้างไหมว่า ชื่อของไวรัสที่เห็นทั่วไปนั้นมีความหมายว่าอย่างไร ทำไมบริษัทที่พัฒนาโปรแกรมป้องกันไวรัสจึงตั้งชื่อแตกต่างกันไป ทั้งๆ ที่ไวรัสที่ค้นพบนั้นเป็นตัวเดียวกัน อย่างไรก็ตามแม้ว่าชื่อจะเขียนไม่เหมือนกันทุกตัวอักษร แต่ความหมายที่แปลได้จากชื่อนั้นเหมือนกัน ตัวอย่างเช่น W32.Klez.h@mm W32/Klez.h@MM WORM_KLEZ.H I-Worm.Klez.h เป็นต้น วิทยานิพนธ์ฉบับนี้จะอธิบายถึงส่วนต่างๆ ของชื่อไวรัส เพื่อทำให้ผู้อ่านสามารถจำแนกแยกแยะประเภทของไวรัสจากชื่อของไวรัส ความสามารถเด่นๆ ตลอดจนวิธีการแพร่กระจายตัวของไวรัสได้

ส่วนประกอบของชื่อไวรัสนั้นแบ่งได้เป็นส่วนๆ ดังนี้



รูปที่ 1.1 แสดงส่วนประกอบต่างๆ ของชื่อไวรัส

1. **ส่วนแรกแสดงชื่อตระกูลของไวรัส (Family_Names)** ส่วนใหญ่จะตั้งตามชนิดของปัญหาที่ไวรัสก่อขึ้น หรือภาษาที่ใช้ในการพัฒนา เช่น เป็นม้าโทรจัน ถูกพัฒนาด้วย Visual Basic scripts หรือเป็นไวรัสที่รันบนระบบปฏิบัติการวินโดวส์ 32 บิต เป็นต้น ซึ่งชื่อของตระกูลของไวรัสที่ค้นพบในปัจจุบันตามตารางที่ 1

ตารางที่ 1.1 แสดงรายชื่อตระกูลของไวรัส

Family Names	ความหมาย
WM	ไวรัสที่เป็นมาโครของโปรแกรม Word
W97M	ไวรัสที่เป็นมาโครของโปรแกรม Word 97
XM	ไวรัสที่เป็นมาโครของโปรแกรม Excel
X97M	ไวรัสที่เป็นมาโครของโปรแกรม Excel 97
W95	ไวรัสที่มีผลกระทบกับระบบปฏิบัติการวินโดวส์ 95
W32/Win32	ไวรัสที่มีผลกระทบกับระบบปฏิบัติการวินโดวส์ 32 บิต
WNT	ไวรัสที่มีผลกระทบกับระบบปฏิบัติการวินโดวส์ NT 32 บิต
I-Worm/Worm	หนอนอินเทอร์เน็ต
Trojan/Troj	ม้าโทรจัน
VBS	ไวรัสที่ถูกพัฒนาด้วย Visual Basic Script
AOL	ม้าโทรจัน America Online
PWSTEAL	ม้าโทรจันที่มีความสามารถในการขโมยรหัสผ่าน
Java	ไวรัสที่ถูกพัฒนาด้วยภาษาจาวา
Linux	ไวรัสที่มีผลกระทบกับระบบปฏิบัติการลินุกซ์
Palm	ไวรัสที่มีผลกระทบกับระบบปฏิบัติการ Palm OS
Backdoor	เปิดช่องให้ผู้บุกรุกเข้าถึงเครื่องได้
HILLW	บ่งบอกว่าไวรัสถูกคอมไพล์ด้วยภาษาระดับสูง

2. ส่วนชื่อของไวรัส (Group_Name) เป็นชื่อดั้งเดิมที่ผู้เขียนไวรัสเป็นคนตั้ง โดยปกติจะถูกแทรกไว้อยู่ในโค้ดของไวรัส และในส่วนนี้เองจะเอามาเรียกชื่อไวรัสเปรียบเสมือนเรียกชื่อเล่น ตัวอย่างเช่น ชื่อของไวรัสคือ W32.Klez.h@mm และจะถูกเรียกว่า Klez.h เพื่อให้สั้นและกระชับขึ้น

3. ส่วนของ Variant รายละเอียดส่วนนี้จะบอกว่าสายพันธุ์ของไวรัสชนิดนั้นๆ มีการปรับปรุงสายพันธุ์จนมีความสามารถต่างจากสายพันธุ์เดิมที่มีอยู่ variant มี 2 ลักษณะคือ

- **Major_Variants** จะตามหลังส่วนชื่อของไวรัส เพื่อบ่งบอกว่ามีความแตกต่างกันอย่างชัดเจน เช่น หนอนชื่อ VBS.LoveLetter.A (A เป็น Major_Variant) แตกต่างจาก VBS.LoveLetter อย่างชัดเจน

- **Minor_Variants** ใช้บ่งบอกในกรณีที่แตกต่างกันนิดหน่อย ในบางครั้ง Minor_Variant เป็นตัวเลขที่บอกขนาดไฟล์ของไวรัส ตัวอย่างเช่น W32.Funlove.4099 หนอนชนิดนี้มีขนาด 4099 KB.

4. ส่วนท้าย (Tail) เป็นส่วนที่จะบอกว่าวิธีการแพร่กระจาย ประกอบด้วย

- **@M หรือ @m** บอกให้รู้ว่าไวรัสหรือหนอนชนิดนี้เป็น "mailer" ที่จะส่งตัวเองผ่านทางอีเมล์เมื่อผู้ใช้ส่งอีเมล์เท่านั้น

- **@MM หรือ @mm** บอกให้รู้ว่าไวรัสหรือหนอนชนิดนี้เป็น "mass-mailer" ที่จะส่งตัวเองผ่านทุกอีเมล์แอดเดรสที่อยู่ในเมล์บอกซ์

ตัวอย่าง W32.HILLW.Lovgate.C@mm แสดงว่า

- อยู่ในตระกูลที่มีผลกระทบต่อระบบปฏิบัติการวินโดวส์ 32 บิต และถูกคอมไพล์ด้วยภาษาระดับสูง
- ชื่อของไวรัสคือ Lovgate
- ที่มี variant คือ C
- มีความสามารถในการแพร่กระจายผ่านทางอีเมล์โดยส่งไปยังทุกอีเมล์แอดเดรสที่อยู่ในเมล์บอกซ์

จากส่วนประกอบของชื่อไวรัสที่ได้อธิบายไว้ข้างต้น จะเห็นได้ว่าชื่อของไวรัสนั้นสามารถบอกถึงประเภทของไวรัส ชื่อดั้งเดิมของไวรัสที่ผู้เขียนไวรัสเป็นคนตั้งสายพันธุ์ต่างๆ ของไวรัสที่ถูกพัฒนาต่อไป และวิธีการแพร่กระจายตัวของไวรัสเองด้วย

วิวัฒนาการไวรัส

วิวัฒนาการของภัยคุกคามทางอินเทอร์เน็ตทวีความรุนแรงมากขึ้นทุกปี ย้อนกลับไปเมื่อ 3 ปีที่แล้ว ภัยคุกคามทางอินเทอร์เน็ตที่ก่อกวนคอมพิวเตอร์ ซึ่งมีชื่อเสียงโด่งดังต้องยกให้ตระกูล “ไวรัส” สายพันธุ์ต่าง ๆ ที่ถูกสร้างขึ้น เพื่อก่อกวนอย่างเดียวไม่ส่งผลกระทบกับข้อมูลในเครื่องคอมพิวเตอร์ สามารถใช้ซอฟต์แวร์แอนตี้ไวรัสลบออกได้ แต่ปีที่ผ่านมาวิวัฒนาการของภัยคุกคามทางอินเทอร์เน็ตก้าวเข้าสู่ตระกูล “เวิร์ม” หรือหนอนคอมพิวเตอร์ ซึ่งมีความสามารถในการก่อกวนเครื่องคอมพิวเตอร์มากขึ้น หลบหลีกการตรวจจับของแอนตี้ไวรัสได้ดีขึ้น และก่อกวนข้อมูลในเครื่องคอมพิวเตอร์พร้อมคัดลอกข้อมูลเพื่อทำให้เซิร์ฟเวอร์เต็มได้แม้ในขณะปิดเครื่องและลบออกได้ยาก แพร่กระจายอย่างเร็วจนเป็นที่ขยาดของผู้ใช้คอมพิวเตอร์ไปตาม ๆ กัน ล่าสุด ปี ค.ศ. 2007 ภัยคุกคามทางอินเทอร์เน็ตมีวิวัฒนาการมากขึ้น มาในรูปแบบของภัยคุกคามตระกูล “มัลแวร์” สายพันธุ์ม้าโทรจัน ที่มีความสามารถในการหลบหลีกและก่อกวนข้อมูลในเครื่องคอมพิวเตอร์ให้เจ้าของเครื่องปวดหัวมากขึ้น

จากการเก็บข้อมูลของบริษัทผลิตซอฟต์แวร์แอนตี้ไวรัสคอมพิวเตอร์ “บิทดีเฟนเดอร์” ตั้งแต่เดือน ม.ค. - ต.ค. รวม 10 เดือน พบโทรจันที่เกิดขึ้นใหม่ถึง 20.36% ซึ่งเป็นโทรจันที่ยังไม่มีฐานข้อมูลเพื่อตรวจจับและยังไม่มีซอฟต์แวร์แอนตี้ไวรัสสำหรับจัดการ โดยแนวโน้มพัฒนาการของโทรจันปีหน้า (ค.ศ. 2008) จะเป็นโทรจันที่สร้างขึ้นเพื่อหลบหลีกการดักจับของแอนตี้ไวรัสมากขึ้น และจะมาในรูปแบบของการดาวน์โหลดซึ่งพ่วงเครื่องมือในการขโมยข้อมูลของเหล่าแฮกเกอร์มาด้วย หากพูดให้เห็นภาพต้องบอกว่า เมื่อคอมพิวเตอร์ติดโทรจันก็เท่ากับว่าในเครื่องคอมพิวเตอร์มีเครื่องมือในการขโมยข้อมูลของแฮกเกอร์อยู่ด้วย เมื่อใดก็ตามที่เชื่อมต่ออินเทอร์เน็ต ข้อมูลส่วนตัว อาทิ เลขบัญชีธนาคาร เลขบัตรเครดิตและรหัสบัตรเครดิต ที่เก็บไว้ในเครื่องจะส่งตรงถึงแฮกเกอร์ทันทีนอกจากนี้เซิร์ฟเวอร์ที่เคยมีข้อมูลนิดหน่อยก็จะเต็มในไม่ช้ากระทั่ง เซิร์ฟเวอร์พังในที่สุด นายเจริญศักดิ์ ศักดิ์รัตนอนันต์ ผู้จัดการทั่วไป บริษัท บิทดีเฟนเดอร์ (ประเทศไทย) กล่าวว่า นอกจากการติดไวรัสโดยรู้เท่าไม่ถึงการณ์แล้ว “สแปมเมล์” หรือ อีเมลขยะ ที่ผู้รับไม่พึงประสงค์ ซึ่งเนื้อหาของสแปมเมล์ที่ถูกส่งมากที่สุด 42.5% คือ การขายยาไวอากร้า ที่พลิกแพลงรูปแบบหลบหลีกการตรวจจับของซอฟต์แวร์แอนตี้ไวรัส โดยมาในรูปของไฟล์ภาพ (image) แบบเอียงๆ และเป็นข้อมูลที่ต่างจากไฟล์ข้อมูลทั่วไป นอกจากนี้ 13.8% เป็นสแปมเมล์เกี่ยวกับการลดน้ำหนัก แม้อีเมล์ขยะจะไม่ทำให้เครื่องพังเหมือนโทรจัน แต่ก็ทำให้เนื้อที่ในการรับจดหมายอิเล็กทรอนิกส์เต็มโดยไม่จำเป็น ทั้งนี้อย่าชะล่าใจคิดว่าคอมพิวเตอร์ที่ใช้งานกันอยู่นั้นจะปลอดภัยจากไวรัส เพราะการสำรวจพบว่า 90% ของเครื่องคอมพิวเตอร์ที่ติดไวรัสมาจากพาหะที่เรียกว่า “ทัมไดรฟ์” วิธีง่าย ๆ ในการตรวจสอบว่าเครื่องคอมพิวเตอร์ติดไวรัสหรือไม่ ให้กดปุ่ม Alt + Ctrl + Delete พร้อมกันทั้ง 3 ปุ่ม ในขณะที่เชื่อมต่ออินเทอร์เน็ตและยังไม่ได้เปิดใช้งานอื่นใด หากพบว่าเนื้อที่ในเซิร์ฟเวอร์ถูกใช้ไปมากทั้งที่ไม่ได้เปิดอย่างอื่นใช้งาน ให้เข้าใจได้เลยว่าเครื่องคอมพิวเตอร์ของคุณติดไวรัสแล้ว! นายเจริญศักดิ์ บอกว่า ความน่ากลัวของภัยคุกคามทางอินเทอร์เน็ต การเติบโตของการใช้งานเครื่องคอมพิวเตอร์ และอินเทอร์เน็ต จะส่งผลให้ปีหน้าบริษัทต่าง ๆ รวมถึงผู้ใช้คอมพิวเตอร์ตามบ้านหันมาให้ความสนใจป้องกันไวรัสคอมพิวเตอร์มากขึ้น ทำให้ตลาดซอฟต์แวร์แอนตี้ไวรัสปีหน้าโตมากกว่าปีนี้ 5 เท่า ซึ่งบิทดีเฟนเดอร์ได้ทุ่มงบพัฒนาซอฟต์แวร์แอนตี้ไวรัสโดยใช้เทคโนโลยีชั้นสูงในการตรวจจับไวรัสและอัพเดทข้อมูลทุกชั่วโมงมากกว่า 2 เท่าของปีนี้ ล่าสุด บิทดีเฟนเดอร์ เปิดตัวซอฟต์แวร์แอนตี้ไวรัสเวอร์ชั่นภาษาไทยเพื่อให้ง่ายต่อการใช้งาน ซึ่งประเทศไทยเป็นประเทศแรกในเอเชียที่มีซอฟต์แวร์แอนตี้ไวรัสของบิทดีเฟนเดอร์ที่เป็นภาษาท้องถิ่น โดยขณะนี้บิทดีเฟนเดอร์ทำซอฟต์แวร์แอนตี้ไวรัสภาษาท้องถิ่นแล้วกว่า 18 ภาษา มีคุณสมบัติในการแอนตี้ไวรัส, สปายแวร์, ฟิชชิ่ง, สแปมเมล์, ไฟร์วอลล์ และมีคุณสมบัติของเกมเมอร์โมด (Gamer Mode) ช่วยให้เล่นเกมได้สบายขึ้น และมีพาเรนทัล คอนโทรล (Parental Control) ช่วยในการป้องกันการเข้าถึงข้อมูลที่สำคัญ ส่วน Total Security มีคุณสมบัติเช่นเดียวกับที่กล่าวมา โดยเพิ่มในส่วนของฟีเจอร์ Tune-Up การควบคุม, ลบ, เรียกคืนไฟล์ และ Back-Up การเรียกคืนข้อมูลและเก็บข้อมูลเก่า

1.2 ความมุ่งหมายและวัตถุประสงค์ของการศึกษา

เนื่องมาจากหลักการที่กล่าวไว้ในในหัวข้อที่ผ่านมาวิทยานิพนธ์ฉบับนี้จะเน้นในเรื่องการวิเคราะห์ข้อมูลของการดาวน์โหลดมัลแวร์/บ็อทในประเทศญี่ปุ่น โดยอาศัยล็อกข้อมูล CCC (Cyber Clean Center) ของปี ค.ศ.2010 และ 2011 เพื่อใช้ตรวจสอบพฤติกรรมต่างๆ ของมัลแวร์/บ็อท

ซึ่งวิทยานิพนธ์ฉบับนี้จะพิจารณาการดาวน์โหลดแบบรายชั่วโมงและรายวันรวมถึงข้อมูลของหมายเลขไอพี แอดเดรสต้นทางที่มัลแวร์/บ็อทใช้งานร่วมกัน

1.3 สมมุติฐานของการวิจัย

เครื่องคอมพิวเตอร์ของผู้ใช้ตามบ้าน หรือในบางองค์กรในประเทศไทย ขณะนี้มากกว่า 50,000 เครื่อง กำลังถูกแฮกเกอร์ครอบครองและแปรสภาพเครื่องดังกล่าวเป็น "Bots", "Zombies" หรือ "Drones" กล่าวคือกลายเป็นเครื่องที่แฮกเกอร์สามารถควบคุมได้จากระยะไกล

โดยเรียกเครื่องคอมพิวเตอร์ที่ถูกแฮกเกอร์ควบคุมว่า "BOTNET" หรือ "Robot Network" กลายเป็นเครือข่ายของแฮกเกอร์เพื่อใช้ในการประกอบกิจกรรมที่ขัดต่อกฎหมาย เช่น ส่งสแปมเมล์ หรือเป็นฐานในการโจมตีเป้าหมายโดยวิธี Denial of Service (Dos Attack) เป็นต้น ซึ่งคาดว่าการแพร่กระจายและการติดมัลแวร์/บ็อทจะเป็นช่วงต้นปีงบประมาณของประเทศญี่ปุ่น หรือช่วงปีใหม่ หรือช่วงเทศกาลสำคัญต่างๆ ซึ่งผู้ใช้งานอาจไม่ได้ใส่ใจการใช้งานคอมพิวเตอร์เท่าที่ควร

1.4 ทฤษฎีหรือแนวความคิดที่ใช้ในการวิจัย

วิทยานิพนธ์ฉบับนี้จะทำการตรวจสอบพฤติกรรมการดาวน์โหลดมัลแวร์/บ็อทจากข้อมูล CCC (Cyber Clean Center) ของปี ค.ศ.2010 และ 2011 โดยจะหาคุณสมบัติของล็อกข้อมูลได้จากสมการตามบทที่ 3 เรื่องวิธีการและเครื่องมือ ทำให้ทราบผลของจำนวนการดาวน์โหลดมัลแวร์/บ็อทรายชั่วโมงและรายวัน เป็นต้น และจะใช้โปรแกรมภาษา R (R Application) ซึ่งเป็นโปรแกรมสำหรับการคำนวณเชิงสถิติ ร่วมกับคำส่ง cat, grep, awk และ sed ในการหา Top-10 มัลแวร์/บ็อท และ Top-10 ประเทศ จากไอพี แอดเดรสของมัลแวร์/บ็อท เป็นต้น

1.5 ขอบเขตการวิจัย

ขอบเขตของการวิจัยในวิทยานิพนธ์ฉบับนี้ จะเป็นการวิเคราะห์ข้อมูลการดาวน์โหลดมัลแวร์/บ็อทในประเทศญี่ปุ่น จากล็อกข้อมูล CCC (Cyber Clean Center) ของปี ค.ศ.2010 และ 2011 ที่ได้จากเครื่อง Honeypots จำนวนมากกว่า 90 เครื่อง บนเครือข่ายหลักลำดับที่ 1 (Japanese Tier-1 Backbone Network) เพื่อใช้ในการตรวจสอบพฤติกรรมต่างๆ ของมัลแวร์/บ็อท โดยจะพิจารณาการดาวน์โหลดมัลแวร์/บ็อทแบบรายชั่วโมงและรายวัน และข้อมูลมัลแวร์/บ็อทที่มาจากไอพี แอดเดรสซับเน็ตเดียวกัน รวมถึงข้อมูลของหมายเลขไอพี แอดเดรสต้นทางที่มัลแวร์/บ็อทใช้งานร่วมกัน

1.6 ขั้นตอนการวิจัย

ขั้นตอนที่ใช้ในการทำวิจัยวิทยานิพนธ์ฉบับนี้ แบ่งขั้นตอนการศึกษาเป็น 5 บท โดยในบทแรกนั้นจะเป็นเนื้อหาเกี่ยวกับความเป็นมาและสาเหตุของปัญหา หลักการหรือแนวคิดในการวิจัยและขอบเขตของงานวิจัย อีก 4 บท สามารถแบ่งเนื้อหาโดยสรุปได้ดังนี้

บทที่ 2 กล่าวถึงความรู้พื้นฐานที่เกี่ยวกับบ็อทเน็ต การติดบ็อทเน็ต การแพร่กระจายของบ็อทเน็ต และรูปแบบการโจมตีของบ็อทเน็ต รวมถึงการดำเนินงานและหน้าที่ของ CCC (Cyber Clean Center)

บทที่ 3 จะเป็นการกล่าวถึงวิธีการและเครื่องมือที่ใช้ในการวิเคราะห์ผลการดาวน์โหลดมัลแวร์/บ็อทแบบรายชั่วโมง รายวัน และจำนวนไอพี แอดเดรสของมัลแวร์/บ็อทที่มาจากต้นทางเดียวกัน

บทที่ 4 เป็นผลงานวิจัย การวิเคราะห์ผลงานวิจัยในส่วนของการดาวน์โหลด Top-10 มัลแวร์/บ็อท แบบรายชั่วโมงและแบบรายวัน รวมถึงค่านอร์มัลไลซ์ของการดาวน์โหลดมัลแวร์/บ็อท และ Top-10 มัลแวร์/บ็อทที่มาจากไอพี แอดเดรสซับเน็ตเดียวกัน ของปี ค.ศ.2010 และ 2011

บทที่ 5 เป็นการสรุปผลการวิจัยและข้อเสนอแนะ

บทที่ 2

บ็อทเน็ต (Botnet) และชุดข้อมูล CCC (Cyber Clean Center)

จากการบังคับใช้ พรบ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เมื่อวันที่ 19 กรกฎาคม 2550 ที่ผ่านมา ทำให้หลายคนต้องระมัดระวังในการใช้งานอินเทอร์เน็ตมากขึ้น เนื่องจาก พรบ. ได้กำหนดบทลงโทษผู้ที่ใช้งานคอมพิวเตอร์ในทางมิชอบ ไม่ว่าจะเป็นการเจาะระบบ, การส่งสแปมเมล์ หรือการส่งต่อข้อมูลที่ไม่เหมาะสม และทำให้ผู้อื่นเสียหาย เป็นต้น ปัญหาที่อาจจะเกิดขึ้นตามมาอย่างหลีกเลี่ยงไม่ได้ก็คือ ถ้าหากมีผู้ใช้งานคอมพิวเตอร์ที่รู้เท่าไม่ถึงการณ์ หรือเครื่องคอมพิวเตอร์ไม่มีระบบความปลอดภัยที่เพียงพอ อาจตกเป็นเหยื่อของแฮกเกอร์เข้ามายึดเครื่องคอมพิวเตอร์นั้นและเข้ามาทำการควบคุมสั่งการให้คอมพิวเตอร์ของเราทำในสิ่งผิดกฎหมายตามที่แฮกเกอร์ต้องการ เช่น การส่งสแปมเมล์ เป็นต้น ทำให้ผู้ใช้คอมพิวเตอร์ดังกล่าว ซึ่งส่วนใหญ่เป็นผู้ใช้งานตามบ้านที่เชื่อมต่อกับระบบอินเทอร์เน็ตความเร็วสูง หรือ ADSL Broadband Internet อาจตกเป็นผู้ต้องหา หรือ “แพะรับบาป” โดยไม่รู้ตัวว่าเครื่องของตนเองได้กลายสภาพเป็นเครื่องของแฮกเกอร์ไปเรียบร้อยแล้ว

ดังนั้น พนักงานเจ้าหน้าที่ หรือ “Forensic Examiner” จึงมีความจำเป็นที่จะต้องมีความรู้ความเข้าใจปัญหาดังกล่าว และสามารถแยกแยะได้ว่าผู้ใช้งานคอมพิวเตอร์ตามบ้านนั้นเป็นเพียงแค่ “เหยื่อ” ของแฮกเกอร์ และไม่ได้มีเจตนาในการกระทำผิดแต่อย่างใด พนักงานเจ้าหน้าที่ตาม พรบ. การกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ต้องผ่านการฝึกอบรมความรู้ด้านการพิสูจน์หลักฐานทางคอมพิวเตอร์ หรือ “Computer Forensic” ในระดับสูงเพื่อที่จะเพิ่มทักษะในการพิสูจน์หลักฐาน และสามารถปฏิบัติภารกิจโดยไม่เกิดปัญหาดังที่กล่าวมาแล้วในตอนต้น

เครื่องคอมพิวเตอร์ของผู้ใช้ตามบ้าน หรือในบางองค์กรในประเทศไทย ขณะนี้มากกว่า 50,000 เครื่อง กำลังถูกแฮกเกอร์ครอบครองและแปรสภาพเครื่องดังกล่าวเป็น “บ็อท” (bots), “ซอมบี้” (zombies) หรือ “โดรน” (drones) กล่าวคือ กลายเป็นเครื่องที่แฮกเกอร์สามารถควบคุมได้จากระยะไกล เราเรียกเครื่องคอมพิวเตอร์หลาย ๆ เครื่องที่ถูกแฮกเกอร์ควบคุมว่า “บ็อทเน็ต” (BOTNET) หรือ “โรบ็อท เน็ตเวิร์ค” (Robot Network) กลายเป็นเครือข่ายของแฮกเกอร์เพื่อใช้ในการประกอบกิจกรรมที่ขัดต่อกฎหมาย เช่น ส่งสแปมเมล์ หรือเป็นฐานในการโจมตีเป้าหมายโดยวิธี Denial of Service (Dos Attack) เป็นต้น ในประเทศสหรัฐอเมริกาทาง FBI (Federal Bureau of Investigation) ได้รายงานว่ามีบ็อทถึงหนึ่งล้านเครื่อง และมีรายงานจากบริษัทความปลอดภัยชื่อดังแจ้งว่าใน 6 เดือนที่ผ่านมาตั้งแต่ต้นปี 2549 มีเครื่องที่กลายเป็นบ็อทแล้วทั่วโลกมากกว่าสี่ล้านเครื่องเลยทีเดียว และมีแนวโน้มที่จะเพิ่มขึ้นอีกในปี 2551

ลักษณะมัลแวร์หรือไวรัสมีการทำงานแบ่งเป็นประเภทดังนี้

ม้าโทรจัน (trojan horse) คือ โปรแกรมที่ดูเหมือนจะมีประโยชน์หรือไม่เป็นอันตราย แต่ในตัวโปรแกรมจะแฝงโค้ดสำหรับการใช้ประโยชน์หรือทำลายระบบที่รัน โดยโปรแกรมนี้ส่วนใหญ่จะถูกแนบมากับอีเมล์ และเมื่อดูเผินๆ ก็เป็นโปรแกรมอรรถประโยชน์ทั่วๆ ไป แต่จริงๆ แล้วข้างในจะแฝงส่วนที่เป็นอันตรายต่อระบบเมื่อรันโปรแกรมนี้

เวิร์ม (worm) คุณสมบัติพิเศษของเวิร์ม คือ สามารถแพร่กระจายตัวของมันเองได้โดยอัตโนมัติและไม่ต้องอาศัยโปรแกรมอื่นในการแพร่กระจายไปยังคอมพิวเตอร์เครื่องอื่นๆ ผ่านทางเครือข่ายเวิร์มสามารถทำอันตรายให้กับระบบ เวิร์มบางประเภทสามารถแพร่กระจายตัวเองโดยที่ไม่ต้องอาศัยการช่วยเหลือจากผู้ใช้เลย หรือบางตัวก็อาจแพร่กระจายเมื่อผู้ใช้รันโปรแกรมบางโปรแกรม นอกจากความสามารถในการแพร่กระจายด้วยตัวเองแล้ว เวิร์มยังสามารถทำลายระบบได้อีกด้วย

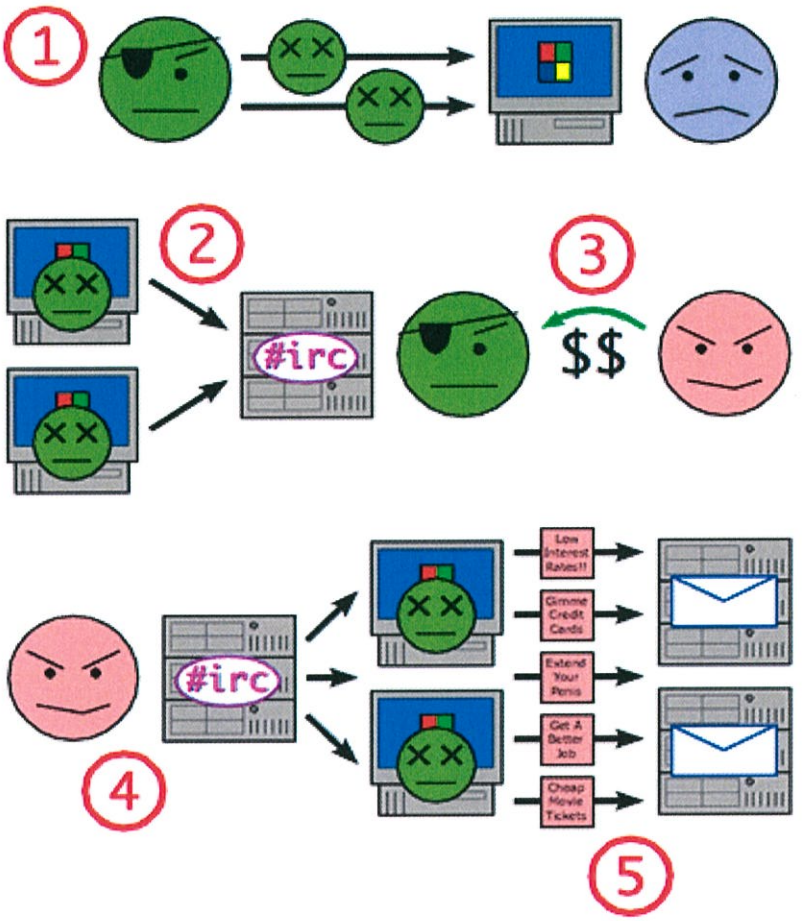
Spyware ไม่แพร่เชื้อไปติดไฟล์อื่นๆ ไม่สามารถส่งตัวเองไปยังคอมพิวเตอร์เครื่องอื่นๆ ได้ ต้องอาศัยการหลอกคนใช้ให้ดาวโหลดเอาไปใส่เครื่องเองหรืออาศัยช่องโหว่ของ web browser ในการติดตั้งตัวเองลงในเครื่องเหยื่อ สิ่งที่มันทำคือรบกวนและละเมิดความเป็นส่วนตัวของผู้ใช้ ส่วนใหญ่จะอยู่ตามเว็บบอร์ดทั่วๆ ไปที่อาจมีเนื้อหาไม่เหมาะสมปนอยู่บ้าง

Phishing เป็นเทคนิคการทำ social engineer โดยใช้อีเมล์เพื่อหลอกให้เหยื่อเปิดเผยข้อมูลการทำธุรกรรมทางการเงินบน อินเตอร์เน็ตเช่น บัตรเครดิตหรือพวก online bank account โดยส่วนใหญ่จะเป็นการสร้างเว็บไซต์ธนาคารแบบปลอม ซึ่งเนียนเหมือนเว็บไซต์ธนาคารจริงๆ เพื่อขโมยพวกเลขที่บัตรเครดิตและรหัสผ่าน ขโมยง่ายๆ เหมือนพวกแฮกเกอร์รอตกปลาผู้ติดเหยื่อในช่วงที่ผู้ที่กำลังเป็นเหยื่อของแฮกเกอร์ใส่รหัสผ่าน

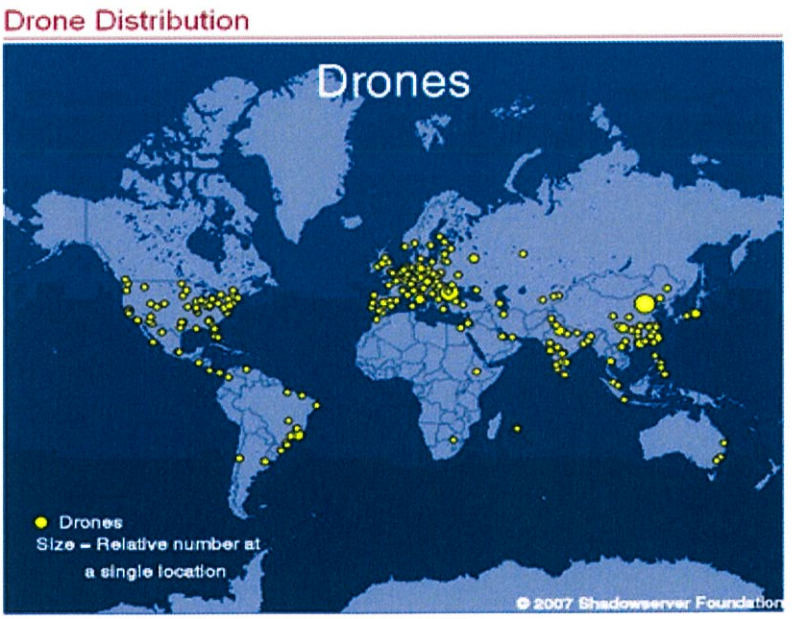
Zombie Network เครื่องคอมพิวเตอร์จำนวนมากๆ จากทั่วโลกที่ตกเป็นเหยื่อของเวิร์ม, ม้าโทรจัน และมัลแวร์อย่างอื่น (compromised machine) ซึ่งจะถูก ผู้โจมตี/แฮกเกอร์ ใช้เป็นฐานปฏิบัติการในการส่ง spam mail, phishing, DoS หรือเอาไว้เก็บไฟล์หรือซอฟต์แวร์ที่ผิดกฎหมาย **Scareware** มักจะปรากฏอยู่ในรูปแบบของผลิตภัณฑ์รักษาความปลอดภัย มีการแจ้งเตือนผู้ใช้ว่ามีการติดเชื้อเกิดขึ้น โดยจะมีการเชื้อเชิญผ่านการโฆษณาบนเว็บว่าติดไวรัส ให้ผู้ใช้ทำการจ่ายเงินเพื่อดาวน์โหลดและติดตั้งตัวโปรแกรม ไม่เพียงเท่านี้ยังส่งผลถึงอันตรายต่อความปลอดภัยของบัตรเครดิตของผู้ใช้และคอมพิวเตอร์อีก ภายในโปรแกรมประเภท scareware มี key logger หรือโทรจันที่ขโมยพาสเวิร์ดอยู่เป็นจำนวนมาก ซึ่งจะเข้าขโมยข้อมูลส่วนบุคคล และยังมีมัลแวร์ตัวอื่นๆ ที่จะส่งผลให้การทำงานของเครื่องผิดปกติไป

ไวรัส (virus) ไวรัสเป็นโปรแกรมที่สามารถติดต่อจากอีกไฟล์หนึ่งไปยังอีกไฟล์หนึ่งภายในระบบ เดียวกัน หรือจากคอมพิวเตอร์เครื่องหนึ่งไปยังเครื่องอื่นโดยการแนบตัวเองไปกับโปรแกรมอื่น มันสามารถทำลายฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูล เมื่อโฮสต์รันโปรแกรมที่ติดไวรัส ส่วนที่เป็นไวรัสก็จะถูกรันด้วยและทำให้แพร่กระจายไปยังเครื่องอื่นหรือบางทีก็สร้างโค้ดใหม่

นี่คือประเภทไวรัสต่างๆ ที่ต้องรับมืออย่างระมัดระวังให้ดี ทั้งในโลกอินเตอร์เน็ต และจากเพื่อนๆ ที่ส่งข้อมูลผ่านทางระบบเครือข่ายในองค์กรหรือส่งมาทาง usb flashdrive ล้วนมีโอกาสติดไวรัสเหล่านี้ทั้งสิ้น อนาคตอาจแพร่ไปยังอุปกรณ์อื่นๆ เช่น โทรศัพท์มือถือสมาร์ทโฟนและแทบเลตด้วย



รูปที่ 2.1 แสดงการทำงานของบ็อทเน็ต จาก WIKIPEPIA.ORG



รูปที่ 2.2 แสดงตำแหน่งของบ็อท หรือ โดรน จาก SHADOWSERVER.ORG

2.1 บ็อท (Bot)

โปรแกรมอัตโนมัติ สำหรับทำหน้าที่อย่างใดอย่างหนึ่งบนอินเทอร์เน็ต ซึ่งย่อมาจากคำว่า โรบ็อท (robot) บ็อทที่นิยมใช้ในอินเทอร์เน็ตสำหรับการเก็บข้อมูลจากเว็บเพจ เรียก เว็บครอว์เลอร์ (web crawler) หรือ สไปเดอร์ (spider) ทำหน้าที่เก็บข้อมูลของเว็บนั้นมาทำการวิเคราะห์ เช่น กูเกิลบ็อท (GoogleBot) เก็บข้อมูลจากเว็บต่างๆ แล้วมาทำดัชนีของเว็บ เพื่อใช้ในเสิร์ชเอนจิน (search engine)

บ็อทในไออาร์ซีหรือในเมสเซนเจอร์ เป็นโปรแกรมอัตโนมัติที่ตอบคำถามของผู้ใช้ต่างๆ โดยบ็อทประเภทนี้ จะนำคำถามของผู้ใช้ มาประมวลผลตามเงื่อนไข และเมื่อพบคำตอบที่น่าจะเกี่ยวข้อง จะส่งคำตอบกลับไป หรือถ้าไม่พบคำตอบ จะส่งข้อความว่าไม่เข้าใจในคำถามให้ถามคำถามใหม่ บ็อทประเภทนี้สามารถตอบคำถามได้หลายประเภท รวมถึงการค้นหา ที่อยู่ เบอร์โทรศัพท์ รายงานสภาพภูมิอากาศปัจจุบัน และผลการแข่งขันกีฬา เป็นต้น

เกมบ็อท เป็นโปรแกรมอัตโนมัติที่ทำหน้าที่ในเกม โดยประพฤติตัวเหมือนผู้เล่นคนอื่น โดยในบางครั้งทางผู้จัดทำเกมจัดไว้ เพื่อไว้ช่วยเหลือ หรือตอบคำถามผู้ใช้ทั่วไป และในบางครั้งผู้ใช้เองจะใช้บ็อทประเภทนี้ เล่นเกมแทนตัวผู้เล่นเอง โดยให้คอมพิวเตอร์ประมวลผล และผู้ใช้เฝ้าดูบ็อทเล่นเกมแทน

สาเหตุที่ผู้ใช้คอมพิวเตอร์ทั่วไปตกเป็นเหยื่อของการโจมตีด้วยบ็อทเน็ตก็คือ การที่ผู้ใช้คอมพิวเตอร์ไม่ได้ติดตั้งซอฟต์แวร์ไฟร์วอลล์ ซึ่งโดยปกติใน Windows XP service Pack 2 ก็จะมีโปรแกรมไฟร์วอลล์ของวินโดวส์ (Windows Firewall) มาให้อยู่แล้ว เพียงแค่เปิดใช้งาน (Enable) ก็จะสามารถป้องกันภัยของบ็อทเน็ตได้ดีในระดับหนึ่ง ปัญหาอีกเรื่องก็คือ ผู้ใช้คอมพิวเตอร์มักจะไม่ค่อยแพตช์ (Patch) ระบบปฏิบัติการที่ใช้อยู่ ทำให้เกิดช่องโหว่ (Vulnerability) ที่แฮกเกอร์สามารถใช้เป็นช่องทางในการเข้ายึดเครื่องของเราได้ ดังนั้น การแพตช์ระบบโดยโปรแกรม “Window Update” ก็เป็นสิ่งที่ควรทำเป็นประจำทุกวัน โดยเราสามารถตั้งให้เครื่องดาวน์โหลดแพตช์โดยอัตโนมัติ เวลาที่เรากำลังเปิดเครื่อง เป็นต้น

ปัญหาบ็อทเน็ตกำลังกลายเป็นปัญหาระดับโลก โดยเฉพาะผู้ให้บริการอินเทอร์เน็ตได้รับผลกระทบเต็มๆ กับเรื่องนี้ เนื่องจากไม่สามารถให้บริการลูกค้าที่กลายเป็นบ็อทได้ ทำให้เกิดปัญหาความไม่เข้าใจกันระหว่างลูกค้าและผู้ให้บริการอินเทอร์เน็ตเอง ดังนั้น การให้ความรู้ความเข้าใจ เรื่อง “Security Awareness Training จึงเป็นเรื่องสำคัญอย่างยิ่งยวด เพื่อที่จะบรรเทาปัญหาดังกล่าวและทำให้เกิดความเข้าใจตระหนักถึงภัยบ็อทเน็ตที่กำลังเพิ่มขึ้นอย่างรวดเร็วในขณะนี้ สำหรับองค์กรทั้งภาครัฐและเอกชน ก็เกิดปัญหาบ็อทเน็ตเช่นกัน เนื่องจากเครื่องคอมพิวเตอร์ในระบบเครือข่าย LAN (Local Area Network) ขององค์กรกลายเป็นซอมบี้หรือบ็อท ซึ่งเครื่องดังกล่าวจะส่งข้อมูลแปลกๆ ออกไปยังระบบอินเทอร์เน็ต องค์กรควรมีระบบ Content Filtering หรือ URL Filtering เพื่อคอยดักจับการทำงานของ bots ตลอดจน ควรมีการเฝ้าระวังโดยใช้ CONCEPT ใหม่ที่เรียกว่า “Extrusion Detection” กล่าวคือ การวิเคราะห์ทราฟฟิค (Traffic) ที่ออกมาจากองค์กรไปยังระบบอินเทอร์เน็ตว่ามีทราฟฟิคแปลกปลอมหรือไม่ โดยปกติแล้วผู้ควบคุมบ็อทหรือแฮกเกอร์ จะใช้โพรโทคอล IRC (Internet Relay Chat) ในการสั่งการบ็อทผ่านทางพอร์ท TCP 6665-6669 ซึ่งถ้าองค์กรมีระบบตรวจจับผู้บุกรุกที่

คอยสังเกตพอร์ทดังกล่าว ก็สามารถที่จะรู้ได้ว่ากำลังถูกโจมตีจากภัยของบ็อทเน็ต ดังที่กล่าวมาแล้วในตอนต้น

การป้องกันบ็อทเน็ตที่ดีที่สุดคือ การให้ความรู้ความเข้าใจแก่ผู้ใช้คอมพิวเตอร์ถึงภัยจากบ็อทเน็ตและการสอนวิธีการป้องกันที่ถูกต้องให้กับผู้ใช้คอมพิวเตอร์ เช่น การเปิดใช้งานซอฟต์แวร์ไฟร์วอลล์และการหมั่นอัพเดตแพตช์ด้วยการอัพเดตวินโดวส์ก็สามารถที่จะป้องกันตนเองและองค์กรให้รอดพ้นจากภัยบ็อทเน็ตได้โดยง่าย อีกทั้งยังไม่ต้องเสียเวลาในการอธิบายกับพนักงานเจ้าหน้าที่ ในกรณีที่เครื่องคอมพิวเตอร์ของเรากลายเป็นผู้ต้องสงสัยในการโจมตีเครื่องของผู้อื่น เพราะกฎหมายได้มีบทลงโทษชัดเจนสำหรับแฮกเกอร์ โดยคำนึงถึงเจตนาในการกระทำเป็นหลัก

ดังนั้น การสืบสวนสอบสวนพิสูจน์หลักฐานทางคอมพิวเตอร์จึงจำเป็นต้องมีความละเอียดรอบคอบในการระบุถึงผู้ต้องหาให้ถูกต้องว่าเป็นแฮกเกอร์ที่แท้จริง หรือเป็นแค่เพียง “เหยื่อ” ของภัยบ็อทเน็ตเท่านั้น

2.2 บ็อทเน็ต (Botnet)

จุดเริ่มต้นของบ็อทเน็ต เริ่มต้นจากแฮกเกอร์เขียนโปรแกรมแบบมัลแวร์ เพื่อติดตั้งในเครื่องของเหยื่อก่อน ไม่ว่าจะด้วยวิธีการไหนก็ตาม เพราะว่ามาได้หลากหลายวิธีมาก ขึ้นอยู่กับเทคนิคการแพร่กระจาย แต่ส่วนใหญ่แล้วเครื่องที่ติด จะเกิดจากการที่เครื่องไม่ได้อัพเดตซอร์ฟแวร์ที่ใช้ ก็คือไม่ได้อัพเดตวินโดวส์ หรือเวอร์ชันของ ลีนุกซ์ เพราะว่าสิ่งที่เค้าให้อัพเดต คือสิ่งที่ช่วยอุดรูรั่วต่างๆ ที่มีคนค้นพบ ไม่ใช่แค่การเพิ่มฟังก์ชั่นใหม่อย่างเดียวอย่างที่หลายคนเข้าใจ และอีกเหตุ ก็คือ เครื่องที่ไม่มีไฟร์วอลล์ (firewall) ในเครื่องไม่รอดเช่นกัน

หลังจากที่เครื่องของเหยื่อติดมัลแวร์ไปแล้วเรียบร้อย เครื่องนั้นจะเรียกว่า ซอมบี้ (zombie) โดยแฮกเกอร์จะเป็นหัวหน้าทัพ จากนั้นแฮกเกอร์ก็จะเพิ่มปริมาณซอมบี้ไปเรื่อยๆ ก็คือทำให้ติดมัลแวร์กันเยอะๆ ขึ้นไปเรื่อยๆ ด้วยการแพร่กระจายกันในเครื่องที่มีรูโหว่อย่างที่ได้กล่าวไปแล้ว

ท้ายที่สุด แฮกเกอร์ที่เป็นแม่ทัพ จะมีซอมบี้ในมือเป็นจำนวนมากมายหลายล้านเครื่อง ซึ่งแน่นอนที่สุดก็คือ แม่ทัพสั่งอะไร ซอมบี้เหล่านั้นก็พร้อมจะทำตามอย่างไม่ต้องสงสัย เคยมีเคส เช่น ว่าอยู่ดีๆ เครื่องที่ใช้แล้วเซฟ (save) ไฟล์ไว้ที่หน้าจอ แล้วก็ถูกลบไปเฉยๆ อะไรแบบนี้ นั่นคือเครื่องคุณเป็น 1 ในซอมบี้ไปแล้วเรียบร้อย เพราะว่าเค้าจะสั่งให้เครื่องซอมบี้เหล่านั้นทำอะไรก็ได้ แม้กระทั่งทำลายทิ้งก็ตาม (ลบข้อมูลทั้งหมด)

ทีนี้ เมื่อแม่ทัพได้รับคำสั่ง ก็จะส่งคำสั่งออกไปที่กองทัพซอมบี้ทั้งหมด ให้ออกไปถล่มทีเดียวพร้อมกันเลย เครื่องที่เป็นเป้าหมายก็จะต้องทำงานหนักเพราะว่าต้องเจอกับกองทัพซอมบี้จำนวนมากเข้าโจมตีพร้อมกัน (ก็มากันเป็นล้านเครื่อง) สุดท้ายเครื่องไม่พัง ก็ทำงานไม่ไหวค้างไป หรือได้รับผลกระทบอย่างน้อยอะไรบางอย่างแน่นอน ส่วนการโจมตีน่าจะมีหลายรูปแบบ แต่ไม่ซับซ้อน เช่น สั่งให้กองทัพมาโหลดไฟล์เดียวจากเว็บเว็บหนึ่งที่อยู่ในเครื่อง track วันนึงมาเป็นสิบล้าน โดนต่อเนื่องหลายวันเหมือนกัน กว่าจะแก้ไขและป้องกันออกไป จนไม่มีผลกระทบกับระบบ

2.2.1 การติดบ็อทเน็ต (Botnet)

สามารถติด มัลแวร์ (malicious software) ได้จากหลากหลายรูปแบบ ไม่ว่าจะเป็นการดาวน์โหลด มาเอง หรือจากช่องโหว่ของ web browser หรือจากการรันม้าโทรจันจากโปรแกรมต่างๆ ซึ่งอาจจะมาในอีเมล์ โดยเครื่องที่ถูกติดตั้งมัลแวร์เหล่านี้ จะถูกควบคุมเครื่องจากระยะไกลได้จากแฮกเกอร์ที่ควบคุมโดยโทรจัน สามารถทำลายตัวเอง หรือว่าอัพเดต หรือแก้ไขโมดูล (module) ตัวเองได้อีกด้วย

2.2.2 การแพร่กระจาย

เราจะเรียกบ็อทเน็ตในชื่อ มัลแวร์ (โปรแกรมไม่พึงประสงค์ ซึ่งมีหลากหลายรูปแบบ) โดยบ็อทเน็ตมีหลายรูปแบบเช่นกัน แต่จะทำงานในแบบเฉพาะตัวกันไป และทำงานได้หลากหลายรูปแบบด้วย ขึ้นอยู่กับผู้ที่สร้างมันขึ้นมา

ซึ่งบ็อทเน็ตเราจะใช้อ้างถึงกลุ่มของบ็อท (เช่น IRC bots) โดยหมายถึง กลุ่มเครื่องที่มีมัลแวร์เหล่านี้ทำงานอยู่ในเครื่อง (เรียกอีกชื่อว่า zombie computer) โดย zombie computer เหล่านี้ (มีมากมายหลายหมื่นหลายแสนเครื่อง) จะมีผู้ควบคุมสูงสุด ชื่อว่า "bot herder" หรือ "บ็อทมาสเตอร์ (bot master)" จะควบคุมโดยการส่งคำสั่งมาจากทีไหนก็ได้ในโลก โดยอาศัยเครือข่ายแบบ IRC network ในการส่งคำสั่งต่อ และเครื่องที่เป็นซอมบี้ก็จะรับคำสั่งและทำตามนั้น บ็อทจะแอบรันโดยทำงานติดต่อกับเซิร์ฟเวอร์ (server) โดยอาศัยการรับส่งข้อมูลที่เหมือนกับ IRC, twitter, IM ใช้งานกันอยู่ เพื่อให้ยากในการตรวจจับ ที่ร้ายกว่านั้นก็คือบ็อทสามารถทำงานด้วยการสแกน (scan) หาเหยื่อรายใหม่ได้ด้วยตัวมันเอง (เพราะได้รับคำสั่งมา) เพื่อหาช่องว่างในเครือข่ายที่ใช้งานอยู่ หรือเจาะเข้าไปในกรณีที่รหัสผ่านง่ายๆ

เท่าที่ตรวจสอบดู พบว่า เครื่องที่อยู่ในประเทศไทย มีการโจมตีไม่น้อยเหมือนกัน (เช็คจากไอพี แอดเดรส) แปลว่าคนไทยเอง ก็ยังมีอีกมากที่ละเลยเรื่องเหล่านี้ จริงๆ มันผิดตั้งแต่เลือกใช้ซอฟแวร์ละเมิดลิขสิทธ์แล้ว เพราะว่าวินโดวส์ที่ละเมิดลิขสิทธิ์จะอัพเดตวินโดวส์ หรือ แพตช์ (patch) อะไรไม่ได้ ทำให้เครื่องมีช่องว่าง รูโหว่เต็มไปหมด จริงๆ รูโหว่เหล่านี้มันไม่ได้พึ่งมี มันมีตั้งแต่ตอนติดตั้งวินโดวส์แล้ว เพียงแต่ว่ารูแต่ละรู ใช้เวลาระยะหนึ่งจนกว่าจะมีคนมาพบเจอ ซึ่งใช้เวลามากน้อยไม่เท่ากัน แต่นับวันก็ยิ่งมีคนเจอเยอะขึ้น

2.2.3 รูปแบบการโจมตี

DDOS - Denial-of-service attacks เป็นชื่อเรียกของการที่มีเครื่องจำนวนมากๆ เรียกใช้งานเข้าไปที่เป้าหมายเดียวกันโดยอัตโนมัติ ซึ่งการเรียกใช้งานนี้จะเป็นการเรียกใช้งานที่หนักกว่าการใช้งานตามปกติมากๆ ทำให้ปลายทางตอบสนองไม่ทัน จนกระทั่งทำงานไม่ไหวไปในที่สุด

Adware – จะแสดงข้อความ หรือโฆษณาในเครื่องขึ้นมาเฉยๆ โดยที่เจ้าของเครื่องยังงงว่ามาจากไหน เรายังไม่ได้เปิดโปรแกรมอะไรเลย เป็นต้น หรืออย่างเช่นไปเปลี่ยนป้ายโฆษณาในบางเว็บ ให้ชี้ไปที่อื่น

Spyware - เป็นโปรแกรมที่ทำหน้าที่เก็บข้อมูลของเจ้าของเครื่องแล้วส่งไปให้บ็อทมาสเตอร์ ไม่ว่าจะเป็น รหัสผ่าน รหัสบัตรเครดิต หรือว่าอื่นๆ ก็ได้ทั้งหมด แม้กระทั่งข้อมูลส่วนตัวที่กรอกไป

ด้วยก็ตาม โดยอาจจะเอาไปขายต่อ หรือเอาไปใช้ปลอมตัวตน เพื่อสร้างความเสียหายได้ ตัวอย่างหนึ่ง เช่น Aurora botnet

E-mail spam – เป็นอีเมล์ที่จะส่งออกไปในนามเจ้าของเครื่อง โดยที่เจ้าของเครื่องไม่ได้รู้เรื่องด้วยเลย โดยอาจจะเป็นโฆษณา หรือสร้างความรำคาญ หรือโปรแกรมตัวมันเอง (แพร่เชื่อ)

Click fraud – เป็นการเปลี่ยนเว็บปลายทางที่เจ้าของเครื่องคลิกไปให้ไปเข้าเว็บตามที่บ็อทมาสเตอร์กำหนดไว้

Fast flux - เป็นการใช้ DNS (Domain Name System) ช่วย โดยเปลี่ยน DNS จากเว็บปกติให้ชี้ไปที่เซิร์ฟเวอร์ที่บ็อทมาสเตอร์ต้องการ (ซึ่งได้สร้างเว็บหลอก เหมือนเว็บจริงเอาไว้รออยู่แล้ว)

Brute-forcing – เป็นการสั่งให้เครื่องไปทดสอบล็อกอิน (login) เครื่องอื่นในโพรโทคอล (protocol) ต่างๆ ไม่ว่าจะเป็น FTP, SMTP หรือ SSH

The worm behavior - บ็อทเน็ตบางตัวถูกออกแบบให้ชอนไชไปในเครือข่ายได้ด้วยตัวเอง และจะติดไปเรื่อย

Scareware - เป็นการติดตั้งไวรัส (virus) ลงเครื่อง เช่น แนะนำให้ซื้อโปรแกรมป้องกันไวรัส (anti virus) ปลอมโดยที่ไม่รู้ตัว เพื่อให้เอาโปรแกรมเข้ามาติดตั้งในเครื่อง

การป้องกัน ไม่ให้เครื่องคอมพิวเตอร์ติดมัลแวร์ หรือกลายเป็นซอมบี้ไม่ยากเลย เพียงแค่ใช้วินโดวส์ลิขสิทธิ์ และต่ออินเทอร์เน็ตเพื่ออัพเดตอย่างน้อยเดือนละครั้งเดียวก็เพียงพอ รวมทั้งต้องใช้ซอฟต์แวร์ไฟร์วอลล์ด้วย และต้องไม่ลืมติดตั้งโปรแกรมป้องกันไวรัส พร้อมกดอัพเดตรายชื่อไวรัสใหม่อย่างน้อยเดือนละครั้ง และที่สำคัญที่สุดคือไม่เปิดเว็บที่ไม่รู้จัก และไม่กดติดตั้งไฟล์หรือโปรแกรมอะไรที่คิดว่าน่าจะไม่ปลอดภัย หรือไม่ทราบที่มาแน่ชัด แต่บางครั้งอาจจะโดนหลอกให้ติดตั้งด้วยความสะเพร่าอันนี้โปรแกรมป้องกันไวรัสจะช่วยได้ในระดับหนึ่ง ต้องเลิกใช้ internet explorer version 6 หรือต่ำกว่าด้วย หรือถ้าใช้ version ที่ใหม่กว่าก็ต้องหมั่นอัพเดตด้วยเช่นกัน (ใน version ตัวเอง ก็มีอัพเดตเรื่อยๆ เช่น internet explorer version 8 ก็จะมีการอัพเดตเพื่อปรับความปลอดภัยเรื่อยๆ โดยไม่ใช่การอัพเดตเป็น version 9)

สำหรับผู้ที่ไม่เคยใช้โปรแกรมป้องกันไวรัส หรือใช้แต่ไม่เคยอัพเดตเลย, ใช้วินโดวส์เถื่อนที่ไม่เคยอัพเดตหรือไม่ใช้ไฟร์วอลล์ (firewall) ก็ให้พึงระวังตอนนี้เครื่องอาจจะกลายเป็น 1 ในซอมบี้โดยไม่รู้ตัวไปแล้วก็ได้

2.3 ชุดข้อมูล CCC (Cyber Clean Center) Dataset ปี ค.ศ.2010-2011

CCC ถูกก่อตั้งขึ้นเมื่อเดือน ธันวาคม พ.ศ.2549 โดยกระทรวงแรงงานและกระทรวงอุตสาหกรรมของประเทศญี่ปุ่น โดยมีจุดประสงค์เพื่อลดการติดบ็อทเน็ตในคอมพิวเตอร์ให้ลดลงจนเป็นศูนย์

CCC เป็นโครงการที่ดำเนินงานมาแล้ว 5 ปี ตั้งแต่ปีงบประมาณ 2006-2010 โดยดำเนินงานร่วมกับ Telecom-ISAC Japan, JPCERT/CC, IPA, ผู้ให้บริการอินเทอร์เน็ต 76 ราย (ISPs), ตัวแทนจำหน่ายโปรแกรมป้องกันไวรัสจำนวน 7 ราย และอื่นๆ

CCC ก่อตั้งขึ้นมาเพื่อวิเคราะห์คุณลักษณะของบ็อท ซึ่งกำลังคุกคามอยู่บนอินเทอร์เน็ต และจัดเตรียมข้อมูลในการป้องกันการแพร่กระจายของบ็อทจากเครื่องคอมพิวเตอร์ของผู้ใช้งาน โดย CCC เป็นองค์กรหลักในการกำจัดบ็อทและป้องกันการติดเชื้อจากเครื่องคอมพิวเตอร์ของผู้ใช้งาน

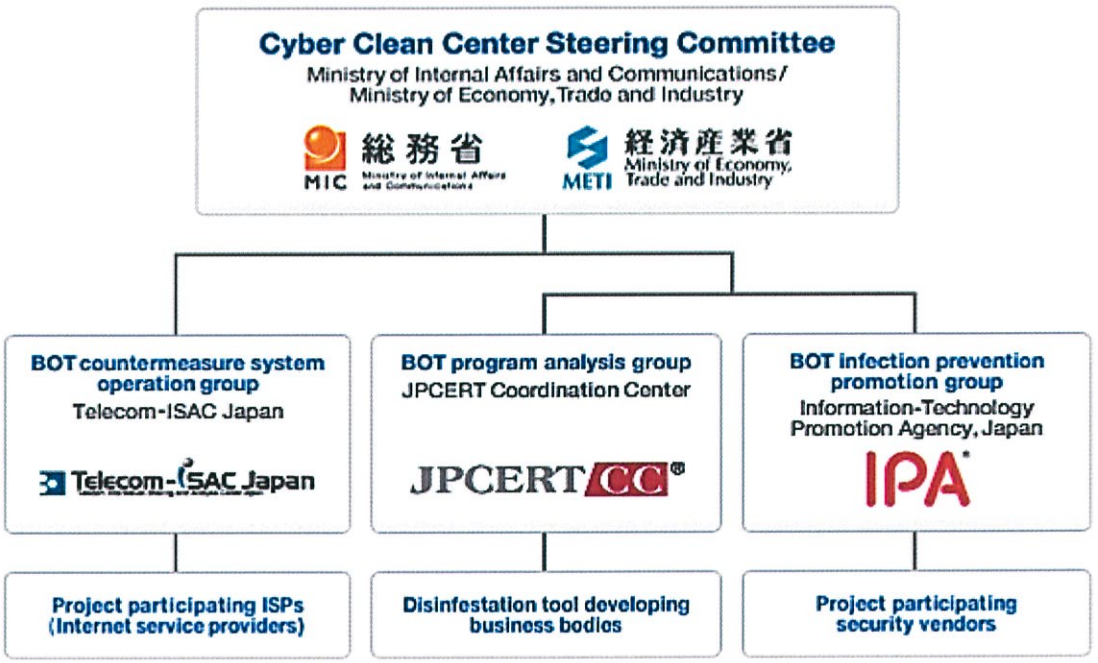
2.3.1 การดำเนินงานและหน้าที่ของ CCC

ภายใต้ Cyber Clean Center-Steering Committee (CCC-SC), CCC ประกอบไปด้วย 3 กลุ่ม ซึ่งครอบคลุมเป้าหมายและกิจกรรมต่างๆ ขององค์กร

ตารางที่ 2.1 หน้าที่หลักของ CCC-SC groups

Bot Countermeasure System Operation Group	ตรวจสอบเครื่องคอมพิวเตอร์ที่ติดเชื้อและแจ้งเตือนผู้ใช้งาน
Bot Program Analysis Group	พัฒนาเครื่องมือเพื่อใช้ในการกำจัดบ็อทเน็ต
Bot Infection Prevention Promotion Group	ป้องกันกิจกรรมที่นำไปสู่การติดบ็อทเน็ต

โครงสร้างการดำเนินงานของ CCC (Cyber Clean Center) เป็นไปตามรูปที่ 2.3



รูปที่ 2.3 โครงสร้างการดำเนินงานของ CCC

1) Bot Countermeasure System Operation Group (Telecom ISAC Japan)

เป็นกลุ่มที่คอยจัดการระบบหลักของโครงการนี้ รวมถึงระบบ ฮันนีพอต (Honeypot) และระบบแจ้งเตือน ซึ่งรวบรวมและวิเคราะห์บ็อท แล้วแจ้งเครื่องคอมพิวเตอร์ของผู้ใช้งานที่ติดบ็อทไปยังผู้ให้บริการอินเทอร์เน็ต (ISPs) โดยมีเป้าหมายในการเรียนรู้ถึงภัยคุกคามรูปแบบใหม่ๆ ของบ็อท ร่วมกับบริษัทตัวแทนจำหน่ายโปรแกรมด้านการรักษาความปลอดภัย

2) Bot Program Analysis Group (JPCERT Coordination Center)

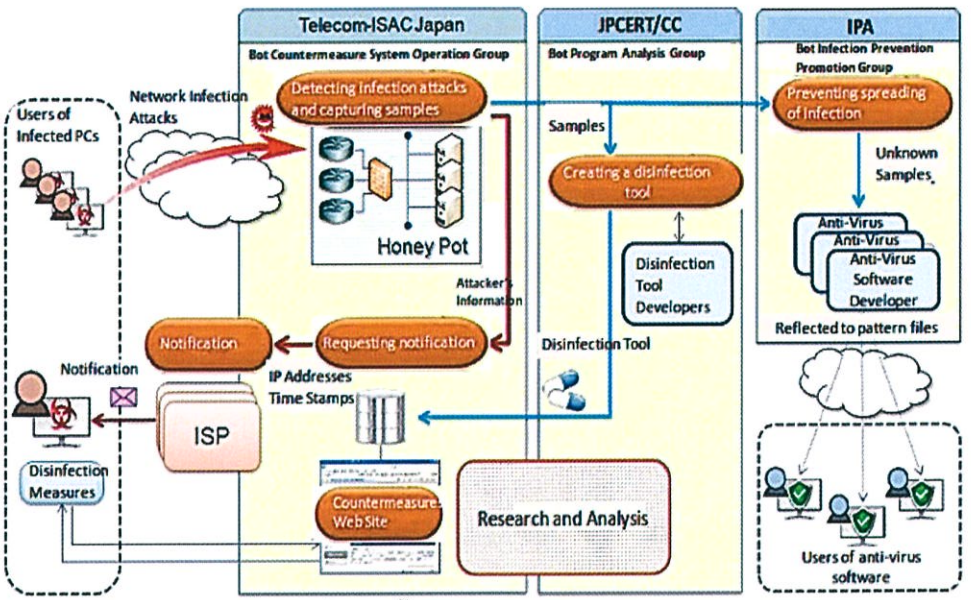
เป็นกลุ่มที่คอยวิเคราะห์คุณลักษณะและเทคโนโลยีการเปลี่ยนแปลงใหม่ๆ ของบ็อทที่ถูกรวบรวมมาจากกลุ่ม Bot Countermeasure System Operation Group โดยกลุ่มนี้จะใช้เครื่องมือในการกำจัดบ็อท และศึกษาวิธีการวิเคราะห์ที่มีประสิทธิภาพร่วมกับบริษัทตัวแทนจำหน่ายโปรแกรมด้านการรักษาความปลอดภัยเพื่อพัฒนาเทคโนโลยีใหม่ๆ ในการป้องกันบ็อท

3) Bot Infection Prevention Promotion Group (Information-Technology Promotion Agency, Japan)

เป็นกลุ่มที่คอยป้องกันการติดเชื้อจากบ็อท รวมถึงการลดความเสี่ยงในการติดเชื้อจากบ็อทลงด้วย

2.3.2 ขั้นตอนการทำงานของ CCC

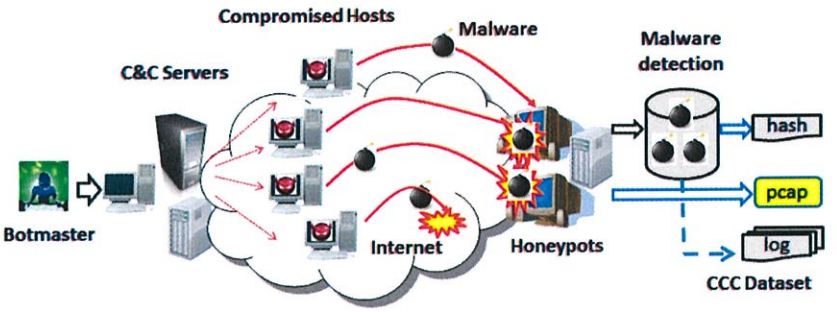
ขั้นตอนการทำงานของ Bot Countermeasure System Operation Group, Bot Program Analysis Group และ Bot Infection Prevention Promotion Group เป็นดังรูปที่ 2.4



รูปที่ 2.4 ขั้นตอนการทำงานของ CCC

2.3.3 การตั้งระบบการวิจัยของ CCC ปี ค.ศ.2010-2011

ในงานวิจัยนี้จะอาศัยล็อกข้อมูลของ CCC ปี ค.ศ.2010-2011 ซึ่งเป็นการตรวจสอบเครื่องฮันนีพอต (Honeypots) จำนวนมากกว่า 90 เครื่องบนเครือข่ายหลักลำดับที่ 1 (Japanese Tier-1 Backbone Network) ดังรูปที่ 2.5 แสดงรูปแบบโครงสร้างที่ใช้ในการทำงานวิจัย โดยเครื่องฮันนีพอตคือเครื่องคอมพิวเตอร์เสมือนที่ติดตั้งระบบปฏิบัติการ Windows XP ที่มีช่องโหว่ให้ผู้บุกรุกสามารถที่จะแฮคได้



รูปที่ 2.5 รูปแบบโครงสร้างของชุดข้อมูล CCC dataset ปี ค.ศ.2010-2011

ข้อมูล CCC ปี ค.ศ.2010 ประกอบด้วยล็อกข้อมูลการดาวน์โหลดของบ็อทเน็ตระหว่างวันที่ 1 พ.ค.2009 – 30 เม.ย.2010 ส่วนของปีค.ศ.2011 ประกอบด้วยล็อกข้อมูลระหว่างวันที่ 1 พ.ค. 2010 – 30 ม.ค.2011 ข้อมูลทั้งสองชุดมีรายละเอียดแสดงในตารางที่ 2.2 โดยเครื่องฮันนีพอต แต่ละเครื่องจะทำการบันทึกแพ็คเก็ตในรูปแบบของ Access Log ซึ่งประกอบด้วยเวลาของการดาวน์โหลด, รหัสของฮันนีพอต, ไอพี แอดเดรสต้นทางและปลายทาง, หมายเลขพอร์ตต้นทางและปลายทาง, ค่าแฮช (Hash Value: SHA1), ชื่อมัลแวร์ และชื่อไฟล์ของมัลแวร์

ตารางที่ 2.2 จำนวนล็อกข้อมูล CCC ปี ค.ศ.2010-2011

รายละเอียด	ปี ค.ศ.2010	ปี ค.ศ.2011
จำนวนเรคคอร์ด	1,162,093	158,734
ใช้โพรโทคอลทีซีพี	1,053,977	136,251
ใช้โพรโทคอลยูดีพี	108,116	22,483
ไอพี แอดเดรส	176,522	82,691
ค่าแฮช (Hash values)	29,858	12,591
ชื่อมัลแวร์ที่ไม่ซ้ำกัน	978	316
จำนวนฮันนีพอต (Honeypots)	92	72
ระยะเวลา	12 เดือน	9 เดือน

2.4 งานวิจัยที่เกี่ยวข้อง

ในการทำงานวิจัยนี้ ผู้จัดทำได้ศึกษาและนำข้อมูลของงานวิจัยอื่นๆ มาวิเคราะห์เพื่อให้ได้ผลงานวิจัยที่สมบูรณ์มากที่สุด ทั้งนี้ได้ศึกษาผลงานวิจัยอื่นๆ จำนวน 4 ผลงาน ดังต่อไปนี้

2.4.1 M.Hatada, Y.Nakatsuru, M.Akiyama and S.Miwa, “Datasets for anti malware research,” IPSJ anti Malware engineering Workshop 2010 (MWS2010), 2010.

งานวิจัยเรื่องนี้ได้นำเสนอว่า มีการทำวิจัยเกี่ยวกับมาตรการการป้องกันมัลแวร์ (malware) มากมายหลายเรื่อง ดังนั้นงานวิจัยนี้จึงทำเรื่อง anti-Malware engineering WorkShop (MWS) คือ ได้จัดทำ MWS 2008 และ MWS 2009 โดยใช้ข้อมูล CCC Dataset ปี ค.ศ.2008 และ 2009 ซึ่งต่างจากงานวิจัยของวิทยานิพนธ์เล่มนี้ ที่ใช้ข้อมูล CCC Dataset ปี ค.ศ.2010 และ 2011

2.4.2 N.R.Rosyid , M.Ohrui, H.Kikuchi, P.Sooraksa and M.Terada, "A discovery of sequential attack patterns of malware in botnets," IEEE International Conference on System Man and Cybermetics (SMC), vol. Vol.2010-CSEC-48, No.37, pp. pp.2564-2570, October 2010.

งานวิจัยเรื่องนี้มีเป้าหมายในการค้นหารูปแบบของการโจมตีแบบใหม่ๆ ของมัลแวร์ ซึ่งไม่ใช่เรื่องง่ายเพราะล็อกข้อมูลมีเป็นจำนวนมาก โดยการแก้ปัญหาของงานวิจัยนี้จะใช้วิธีการ PrefixSpan เพื่อวิเคราะห์รูปแบบการโจมตีของมัลแวร์ และใช้ข้อมูล CCC Dataset ปี ค.ศ.2009

2.4.3 J.Song, J.Shimamura, M.Eto, D.Inoue and K.Nakao "Correlation analysis between spamming botnets and malware infected hosts," in IEEE/IPSJ 11th International Symposium on Applications and the Internet (SAINT), July 2011, pp. pp.372-375.

งานวิจัยเรื่องนี้ได้นำเสนอว่า การโจมตีทางคอมพิวเตอร์โดยบ็อทเน็ต (Botnet) มีเป้าหมายเพื่อโจมตีในวงกว้าง เช่น การส่ง spam email และ DDoS (distributed denial of service) เป็นต้น ในหลายๆ กรณี บ็อทเน็ตจะประกอบด้วยบ็อทหรือ zombie PCs เป็นจำนวนมาก โดยที่มันจะแพร่กระจายไปยังเครื่องเหยื่อบนอินเทอร์เน็ต ดังนั้นการลดความเสียหายจากบ็อทเน็ตจึงต้องเข้าใจรูปแบบโครงสร้างพื้นฐานของบ็อทเน็ต ซึ่งงานวิจัยนี้จะวิเคราะห์ความสัมพันธ์ระหว่าง spamming บ็อทเน็ต จำนวน 10 ชนิด (ได้จากการวิเคราะห์ spam email เป็นเวลา 3 สัปดาห์จากงานวิจัยครั้งก่อน) กับเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ โดยทำการเปรียบเทียบสมาชิก (บ็อท) ของ spammingบ็อทเน็ตกับเครื่องคอมพิวเตอร์ต้นทาง พบว่า 7.2 % - 37.5% ของ spamming บ็อทเน็ตจะติดเชื้อจากมัลแวร์ต่างชนิดกันจำนวน 4 ตัว เป็นอย่างน้อย

2.4.4 K.Sisaat, H.Kikuchi, S.Matsuo, M.Terada, M.Fujiwara and S.Kittitornkun, "Time zone correlation analysis of malware/bot downloads," To be published in IEICE Transactions on Communications, vol. Vol.E96-B, No.07, 2013.

งานวิจัยเรื่องนี้ได้นำเสนอว่า บ็อทเน็ตทำการโจมตีไปยังเครื่องเหยื่อผ่าน C&C Server (Command and Control) ซึ่งถูกควบคุมโดย botmaster โดยทำการวิเคราะห์ไอพี แอดเดรสต้นทางของการดาวน์โหลดจากข้อมูล CCC Dataset ปี ค.ศ.2010 ซึ่งข้อมูลเหล่านี้ได้มาจากเครื่องฮันนีพอตมากกว่า 90 เครื่อง โดยงานวิจัยนี้จะนำเสนอความสัมพันธ์ทางด้านเวลา (Time Zone) ซึ่งเป็นตัวกำหนดความสัมพันธ์ระหว่างการดาวน์โหลดบ็อทจากประเทศญี่ปุ่นกับประเทศอื่นๆ

บทที่ 3
วิธีการและเครื่องมือ

ในบทนี้จะกล่าวถึงการดาวน์โหลดบ็อทเน็ตไบนารี่ ซึ่งบันทึกล็อกข้อมูลเกี่ยวกับกิจกรรมต่างๆ ของบ็อทเน็ตเป็นล้านๆ เรคคอร์ดในประเทศญี่ปุ่น ทั้งนี้จะพิจารณาถึงพฤติกรรมของมัลแวร์/บ็อท โดยดูจากรูปแบบในการดาวน์โหลดบ็อทเน็ต

3.1 โครงสร้างล็อกข้อมูลของ CCC

ล็อกข้อมูลที่จะทำการวิเคราะห์ถูกเก็บในรูปแบบไบนารี่ ซึ่งจะทำการพิจารณา 2 ส่วนใน 1 ชุดข้อมูล โดยใช้ล็อกข้อมูล CCC Dataset ของปี ค.ศ.2010 – 2011 โครงสร้างล็อกข้อมูลใน CCC Dataset ประกอบด้วย 9 ฟิลด์ แต่ละฟิลด์ถูกแยกด้วยเครื่องหมาย , (Comma) ซึ่งจะชี้ให้เห็นถึงรูปแบบการดาวน์โหลดตามพฤติกรรมของบ็อทเน็ตดังตารางที่ 3.1

ตารางที่ 3.1 โครงสร้างล็อกข้อมูลของ CCC

Timestamp	SRC IP	SRC Port	DST IP	DST Port	Protocols	Hash Values	Bot Name	Bot File name
2010-03-01 00:00:08,honey060,1029,202.219.137.24,26794,TCP,9c90793c0bb542a97ae bffbd7c1542f7dce1b247,PE_VIRUT.AV,C:\WINNT\system32\qbssun.exe								

1) Timestamp : เก็บข้อมูลเวลา Phenomenon Time ของการดาวน์โหลดบ็อทของเครื่อง C&C Server และ Honeypots โดยเรียงตามปี เดือน วัน ชั่วโมง นาที และวินาที เช่น 2009-05-01 00:01:05

2) SRC IP : ไอพีต้นทางของบ็อทที่เก็บไบนารี่ ซึ่งจะเกิดช่วงดาวน์โหลดบ็อทระหว่างเซิร์ฟเวอร์กับฮันนีพอต (Honeypots)

3) SRC Port : พอร์ตต้นทางของมัลแวร์/บ็อท ซึ่งมีพอร์ตที่ลงทะเบียนไว้ตั้งแต่ พอร์ตหมายเลข 1024 – 49151 และพอร์ตหมายเลข 49152 - 65535 ตามลำดับ

4) DST IP : ไอพีปลายทาง หรือไอพีเป้าหมายของมัลแวร์/บ็อท หรือเครื่องเหยื่อ (อาจเป็น Honeypots ID)

5) DST Port : พอร์ตที่มีช่องโหว่ของเครื่องโฮสต์ที่ตกเป็นเป้าหมาย ซึ่งใช้ในการเชื่อมต่อ/ดาวน์โหลดมัลแวร์/บ็อท โดยที่ DST Port จะถูกนำมาใช้กับแอพพลิเคชั่นบนเครือข่าย ซึ่งเรียกว่า well-known ports อยู่ในช่วงหมายเลข 1 – 1023

6) Protocols : โพรโทคอลที่ถูกใช้โดยบ็อท ได้แก่ โพรโทคอล TCP และ UDP

7) Hash values (SHA-1) : SHA-1 เป็นตัวแปรสำหรับมัลแวร์/บ็อท ซึ่งบ็อทจะมีค่า Hash values หลากหลาย แตกต่างกัน

8) Name : ชื่อมัลแวร์ได้มาจากสัญลักษณ์ของมัลแวร์ ซึ่งถูกใช้ทางการค้าโดยโปรแกรมป้องกันไวรัส เช่น Trend Micro

9) File name : ชื่อไฟล์สามารถตั้งชื่อได้ไม่ซ้ำกัน

3.2 พฤติกรรมการดาวน์โหลดมัลแวร์

งานวิจัยนี้จะทำการตรวจสอบพฤติกรรมการดาวน์โหลดมัลแวร์จากล็อกข้อมูล CCC ปี ค.ศ.2010 และ 2011 เพื่อวิเคราะห์ล็อกข้อมูลที่เกิดจากการดาวน์โหลดมัลแวร์แต่ละตัวโดยสามารถคำนวณพฤติกรรมให้อยู่ในรูปแบบของจำนวนการดาวน์โหลดรายชั่วโมงหรือรายวันได้ อย่างไรก็ตามตัวแปรของการดาวน์โหลดมัลแวร์มีค่อนข้างมาก ดังนั้นการหาค่านอร์มัลไลซ์ของจำนวนการดาวน์โหลดมัลแวร์เป็นสิ่งที่จะต้องดำเนินการในงานวิจัยนี้

คำนิยามที่ 1 : ให้ $l^{u,v}_{w,x,y}(d, h, m, s)$ เป็นจำนวนการดาวน์โหลดของมัลแวร์ w ซึ่งมาจากไอพีแอดเดรสต้นทาง u, พอร์ตต้นทาง v ไปยังไอพี แอดเดรสปลายทาง x และพอร์ตปลายทาง y ของวันที่ d, ชั่วโมงที่ h, นาทีที่ m และวินาทีที่ s ตามลำดับ ดังนั้นจะสามารถหาคุณสมบัติของล็อกข้อมูลได้ตามสมการเหล่านี้

- จำนวนการดาวน์โหลดมัลแวร์ w ทั้งหมด ณ ชั่วโมงที่ h ของวันใดๆ ใน 1 ปี

$$l_w(h) = \sum_{h=0}^{23} l^{u,v}_{w,x,y}(d, h, m, s), \forall u, \forall v, \forall x, \forall y, \forall m, \forall s \quad (3.1)$$

- จำนวนการดาวน์โหลดมัลแวร์ w ทั้งหมดของวันที่ d :

$$l_w(d) = \sum_{d=1}^{365} l^{u,v}_{w,x,y}(d, h, m, s), \forall u, \forall v, \forall x, \forall y, \forall m, \forall s \quad (3.2)$$

- ค่าเฉลี่ยของการดาวน์โหลดมัลแวร์ w รายชั่วโมง :

$$\bar{l}^{h}_{w} = \frac{\sum_{h=0}^{23} l_w(h)}{24} \quad (3.3)$$

- ค่าเบี่ยงเบนของการดาวน์โหลดมัลแวร์ w รายชั่วโมง :

$$\Delta l_w(h) = l_w(h) - \bar{l}_w(h) \quad (3.4)$$

- จำนวนการดาวน์โหลดมัลแวร์รายชั่วโมงที่สูงที่สุด :

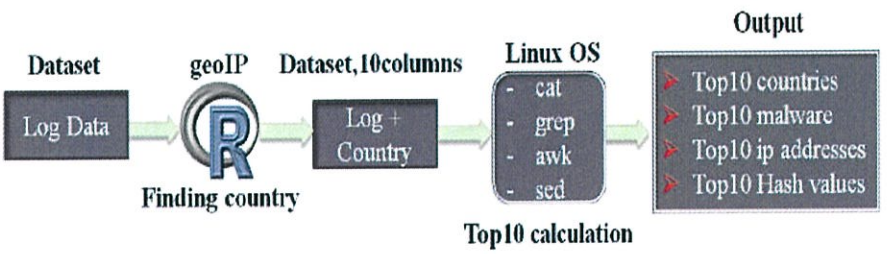
$$\Delta l_w(h)_{max} = \max|\Delta l_w(h)| \quad (3.5)$$

- ค่านอร์มัลไลซ์ของการดาวน์โหลดมัลแวร์ w รายชั่วโมง :

$$\Delta l'_w(h) = \frac{\Delta l_w(h)}{\Delta l_w(h)_{max}} \quad (3.6)$$

3.3 เครื่องมือและอุปกรณ์ที่ใช้ในงานวิจัย

ชุดข้อมูลประกอบด้วยล็อกข้อมูลการดาวน์โหลดมัลแวร์/บ็อทจำนวนมาก ซึ่งประกอบด้วย เวลาของการดาวน์โหลด, ไอพี แอดเดรสต้นทางและปลายทาง, หมายเลขพอร์ตต้นทางและปลายทาง, ค่าแฮช, ชื่อมัลแวร์และชื่อไฟล์ของมัลแวร์ บนพื้นฐานที่ล็อกข้อมูลการดาวน์โหลดมัลแวร์/บ็อท มีจำนวนมาก งานวิจัยนี้จะทำการวิเคราะห์และนับผลรวมของการดาวน์โหลดมัลแวร์แบบชั่วโมง และรายวัน โดยใช้เครื่องมือ ได้แก่ R Application ซึ่งเป็นโปรแกรมฟรี สามารถโหลดมาใช้งานได้โดย ไม่มีค่าใช้จ่าย ซึ่งใช้สำหรับการคำนวณเชิงสถิติ และในการทำงานวิจัยนี้จะใช้คำสั่ง cat, grep, awk และ sed ในการหา Top-10 มัลแวร์/บ็อท, Top-10 ประเทศ และอื่นๆ ตามรูปที่ 3.1



รูปที่ 3.1 การประมวลผลเพื่อหา Top-10 มัลแวร์/บ็อท และอื่นๆ

- geoIP : เป็นคำสั่งที่ใช้ค้นหาชื่อประเทศ ซึ่งงานวิจัยนี้จะนำเข้าล็อกข้อมูลผ่านโปรแกรม R และใช้ฟังก์ชั่นของ geoIP วิเคราะห์ไอพี แอดเดรสต้นทางของมัลแวร์/บ็อทแต่ละตัวเพื่อค้นหาชื่อประเทศ

รูปแบบคำสั่ง geoIP

geoIP(x) โดยที่ x คือค่าไอพี แอดเดรสในรูปแบบ ipV4
เช่น

```
x <- "38.122.8.198"
geoIP(x)
```

```
{
        "statusCode" : "ERROR",
        "statusMessage" : "Invalid API key.",
        "ipAddress" : "XXX.XXX.XXX.XXX",
        "countryCode" : "",
        "countryName" : "",
        "regionName" : "",
        "cityName" : "",
        "zipCode" : "",
        "latitude" : "0",
        "longitude" : "0",
        "timeZone" : ""
}
```


ตารางที่ 3.2 รูปแบบของตัวแปรที่ใช้โดยคำสั่ง geoIP

ตัวแปร	รายละเอียด
IPaddress	ค่าไอพี แอดเดรส
statusCode	ส่งคืนสถานะรหัสหลังจากตรวจพบ
latitude	เส้นละติจูด
longtitude	เส้นลองติจูด
statusMessage	ส่งคืนสถานะข้อความหลังจากตรวจพบ
countryCode	รหัสประเทศ จากการตรวจสอบไอพี แอดเดรส
countryName	ชื่อประเทศ จากการตรวจสอบไอพี แอดเดรส
regionName	รัฐ/จังหวัด จากการตรวจสอบไอพี แอดเดรส
cityName	เมือง จากการตรวจสอบไอพี แอดเดรส
zipCode	รหัสไปรษณีย์ จากการตรวจสอบไอพี แอดเดรส
TimeZone	เขตเวลา จากการตรวจสอบไอพี แอดเดรส

- cat : เป็นคำสั่งที่ใช้ดูหรือแสดงข้อมูล ซึ่งงานวิจัยนี้ใช้ในการรวมข้อมูลแต่ละเดือนในหนึ่งปีให้เป็นไฟล์เดียวกัน

รูปแบบคำสั่ง cat

cat [options] [files]

เช่น

$ cat /etc/passwd

$ cat /etc/passwd > /tmp/test.txt

$ cat /etc/hosts /etc/resolv.conf /etc/fstab

$ cat /etc/hosts /etc/resolv.conf /etc/fstab > /tmp/outputs.txt
$ cat /tmp/outputs.txt

- awk : เป็นภาษาโปรแกรมที่ออกแบบมาเพื่อประมวลผลข้อความในไฟล์หรือสตรีม ซึ่งงานวิจัยนี้ใช้ในการนับและหามัลแวร์, ไอพี แอดเดรส, ประเทศ และอื่นๆ

รูปแบบคำสั่ง awk

awk 'BEGIN {start_action} {action} END {stop_action}' filename
เช่น
awk '{print $1}' input_file
-rw-r--r--
-rw-r--r--
-rw-r--r--
-rw-r--r--
-rw-r--r--
-rw-r--r—

awk '{ if($9 == "t4") print $0;}' input_file
-rw-r--r-- 1 pcenter pcenter 43 Dec 8 21:39 t4

awk 'BEGIN { for(i=1;i<=5;i++) print "square of", i, "is",i*i; }'
square of 1 is 1
square of 2 is 4
square of 3 is 9
square of 4 is 16
square of 5 is 25

- grep : เป็นคำสั่งที่ใช้ในการค้นหาข้อความในไฟล์ ซึ่งงานวิจัยนี้ใช้งานคำสั่งนี้ 2 แบบ แบบแรกใช้ในการหาจำนวนมัลแวร์ในล็อกข้อมูล ส่วนแบบที่สองใช้ในการสร้างและบันทึก Greped Lines เป็นไฟล์ใหม่

รูปแบบคำสั่ง grep

grep 'word' filename
grep 'word' file1 file2 file3
grep 'string1 string2' filename
cat otherfile | grep 'something'
command | grep 'something'
command option1 | grep 'data'

grep --color 'data' filename
เช่น
$ grep boo /etc/passwd
foo:x:1000:1000:foo,,,:/home/foo:/bin/ksh

$ grep -r "192.168.1.5" /etc/
/etc/ppp/options:# ms-wins 192.168.1.50
/etc/ppp/options:# ms-wins 192.168.1.51
/etc/NetworkManager/system-connections/Wired connection 1:addresses1
=192.168.1.5;24;192.168.1.2;

$ grep -h -R "192.168.1.5" /etc/
# ms-wins 192.168.1.50
# ms-wins 192.168.1.51
addresses1=192.168.1.5;24;192.168.1.2;

- sed : เป็นคำสั่งที่ใช้ในการค้นหาข้อความในไฟล์และเปลี่ยนแปลงข้อความนั้นๆ ซึ่งงานวิจัยนี้ใช้ในการกรองเนื้อหาและสัญลักษณ์ก่อนออกมาเป็นผลลัพธ์ที่ต้องการ

รูปแบบคำสั่ง sed

sed *OPTIONS*... [*SCRIPT*] [*INPUTFILE*...]
เช่น
>cat file.txt
unix is great os. unix is opensource. unix is free os.
learn operating system.
unixlinux which one you choose.

>sed 's/unix/linux/' file.txt
linux is great os. unix is opensource. unix is free os.
learn operating system.
linuxlinux which one you choose.

>sed 's/unix/linux/2' file.txt
unix is great os. linux is opensource. unix is free os.
learn operating system.
unixlinux which one you choose.

```
>sed 's/unix/linux/g' file.txt
linux is great os. linux is opensource. linux is free os.
learn operating system.
linuxlinux which one you choose.
```

บทที่ 4
ผลงานวิจัย

ในบทนี้จะกล่าวถึงผลงานวิจัยของการดาวน์โหลดมัลแวร์/บ็อทจากชุดข้อมูล CCC Datasets ของปี ค.ศ.2010-2011

4.1 การวิเคราะห์ผลงานวิจัย

ในส่วนนี้จะสรุปผลของการดาวน์โหลด Top-10 มัลแวร์/บ็อท ของปี ค.ศ.2010-2011 แบบรายชั่วโมง รายวัน และการหาค่านอร์มัลไลซ์ของการดาวน์โหลดรายชั่วโมง

4.1.1 สรุปผลการดาวน์โหลดมัลแวร์/บ็อทของปี ค.ศ.2010-2011

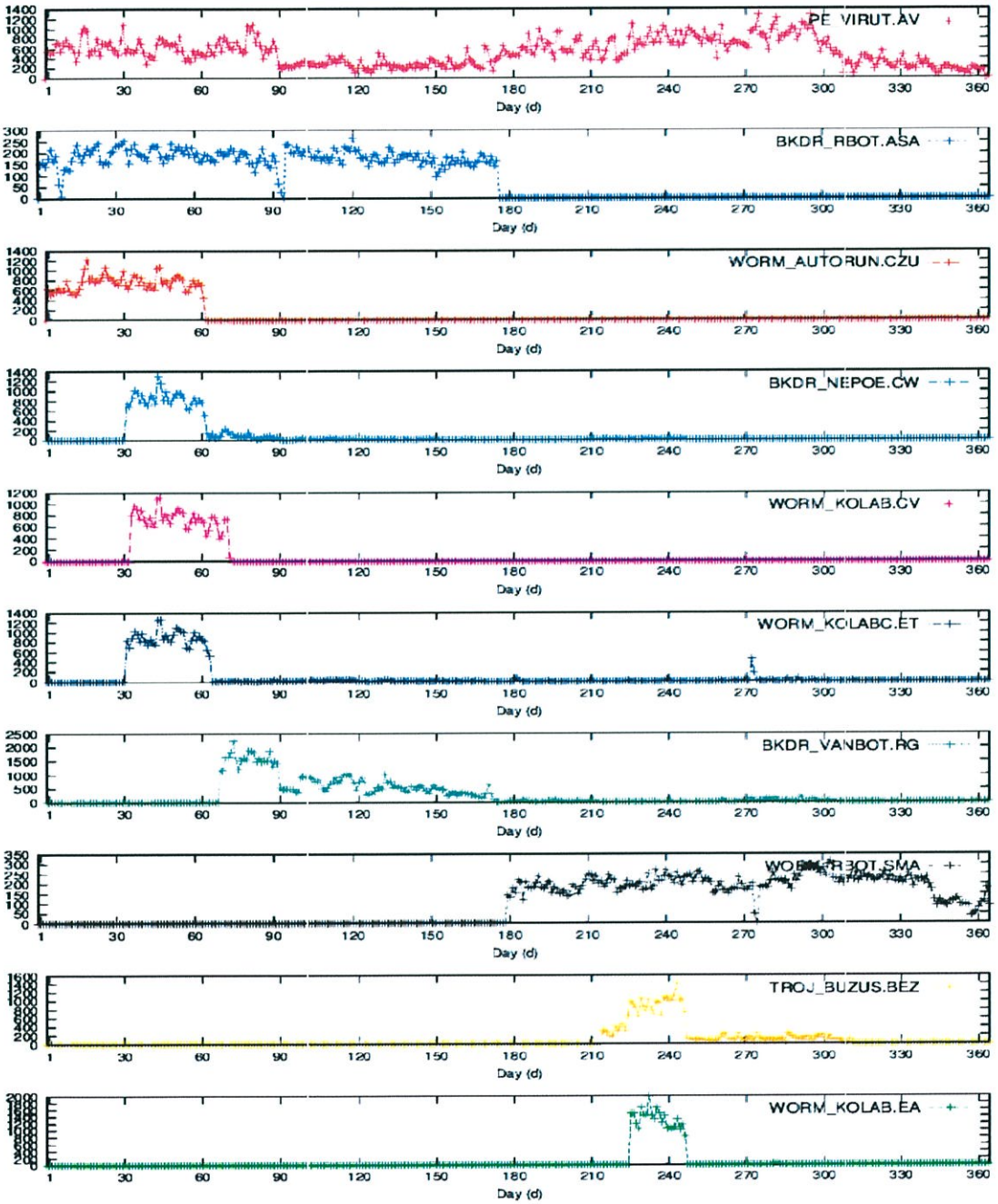
ข้อมูล CCC ปี ค.ศ.2010 ประกอบด้วยล็อกข้อมูลการดาวน์โหลดของบ็อทเน็ตระหว่างวันที่ 1 พ.ค.2009 – 30 เม.ย.2010 ส่วนของปี ค.ศ.2011 ประกอบด้วยล็อกข้อมูลระหว่างวันที่ 1 พ.ค 2010 – 30 ม.ค.2011 ข้อมูลทั้งสองชุดมีรายละเอียดดังแสดงในตารางที่ 4.1

ตารางที่ 4.1 จำนวนล็อกข้อมูล CCC ปี ค.ศ.2010-2011

รายละเอียด	ปี ค.ศ.2010	ปี ค.ศ.2011
จำนวนเรคคอร์ด	1,162,093	158,734
ใช้โปรโตคอลทีซีพี	1,053,977	136,251
ใช้โปรโตคอลยูดีพี	108,116	22,483
ไอพี แอดเดรส	176,522	82,691
ค่าแฮช (Hash values)	29,858	12,591
ชื่อมัลแวร์ที่ไม่ซ้ำกัน	978	316
จำนวนฮันนีพอต (Honeypots)	92	72
ระยะเวลา	12 เดือน	9 เดือน

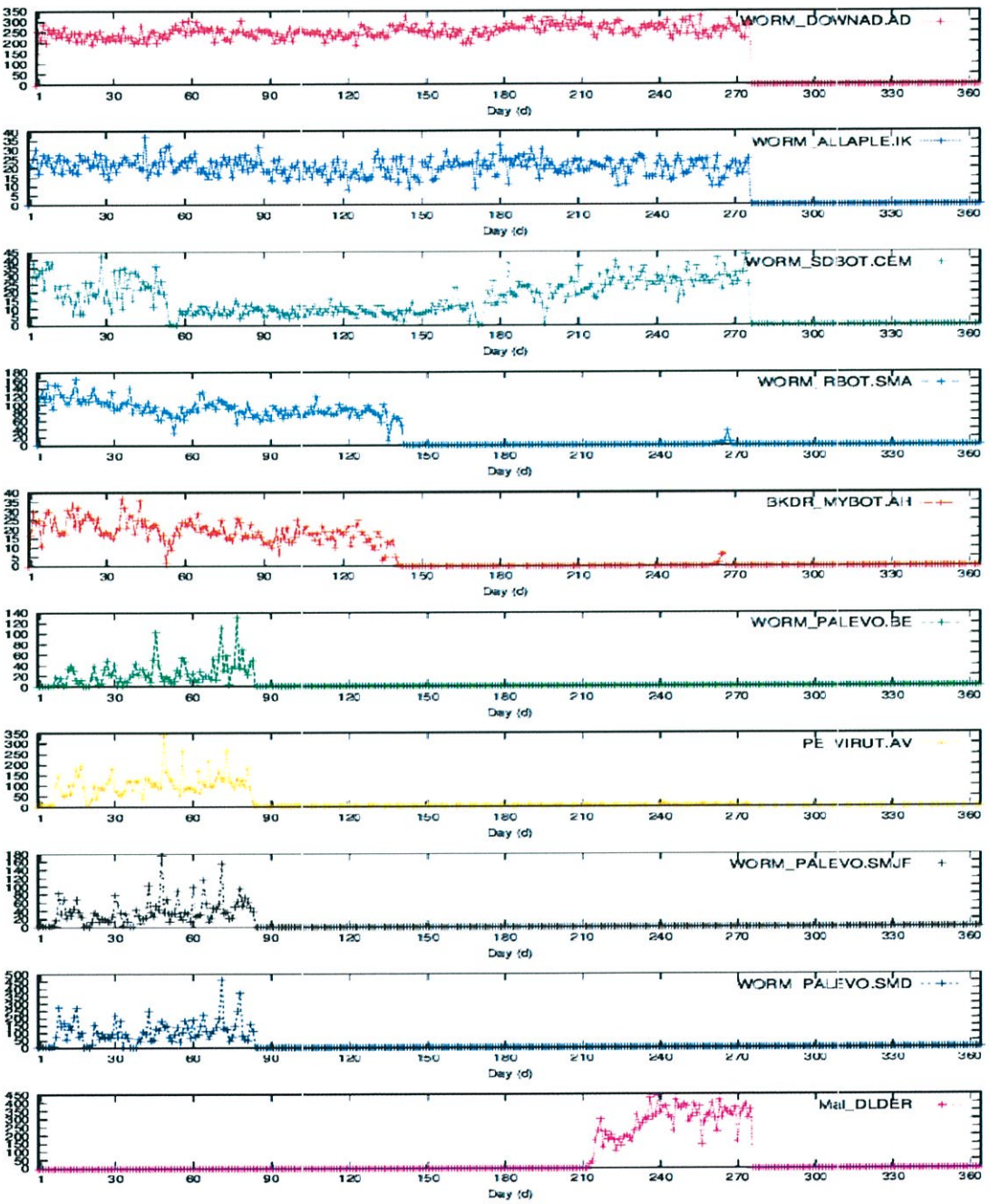
4.1.2 การดาวน์โหลดมัลแวร์/บ็อท แบบรายวันของปี ค.ศ.2010-2011

การดาวน์โหลด Top-10 มัลแวร์/บ็อท แบบรายวันของปี ค.ศ.2010 มีรายละเอียดดังรูปที่ 4.1 ซึ่งในปี ค.ศ.2010 พฤติกรรมการดาวน์โหลดมีความคล้ายคลึงและสัมพันธ์กัน การดาวน์โหลดส่วนใหญ่เป็นช่วงต้นปีงบประมาณของญี่ปุ่น



รูปที่ 4.1 การดาวน์โหลดมัลแวร์/บ็อท แบบรายวันของปี ค.ศ.2010

ส่วนการดาวน์โหลด Top-10 มัลแวร์/บ็อท แบบรายวันของปี ค.ศ.2011 มีรายละเอียดดังรูปที่ 4.2 ซึ่งในปี ค.ศ.2011 จะพบว่า มัลแวร์/บ็อทบางส่วนถูกดาวน์โหลดต่อเนื่องจากปี 2010 มายังปี 2011 เช่น มัลแวร์ชื่อ PE_VIRUT.AV และพบมัลแวร์/บ็อทรายใหม่ๆ เพิ่มมากขึ้น ซึ่งพฤติกรรมการดาวน์โหลดมีความคล้ายคลึงกันบ้างในบางช่วงเวลา



รูปที่ 4.2 การดาวน์โหลดมัลแวร์/บ็อท แบบรายวันของปี ค.ศ.2011

4.1.3 ค่าเฉลี่ยการดาวน์โหลดมัลแวร์/บ็อท รายชั่วโมงของปี ค.ศ.2010-2011

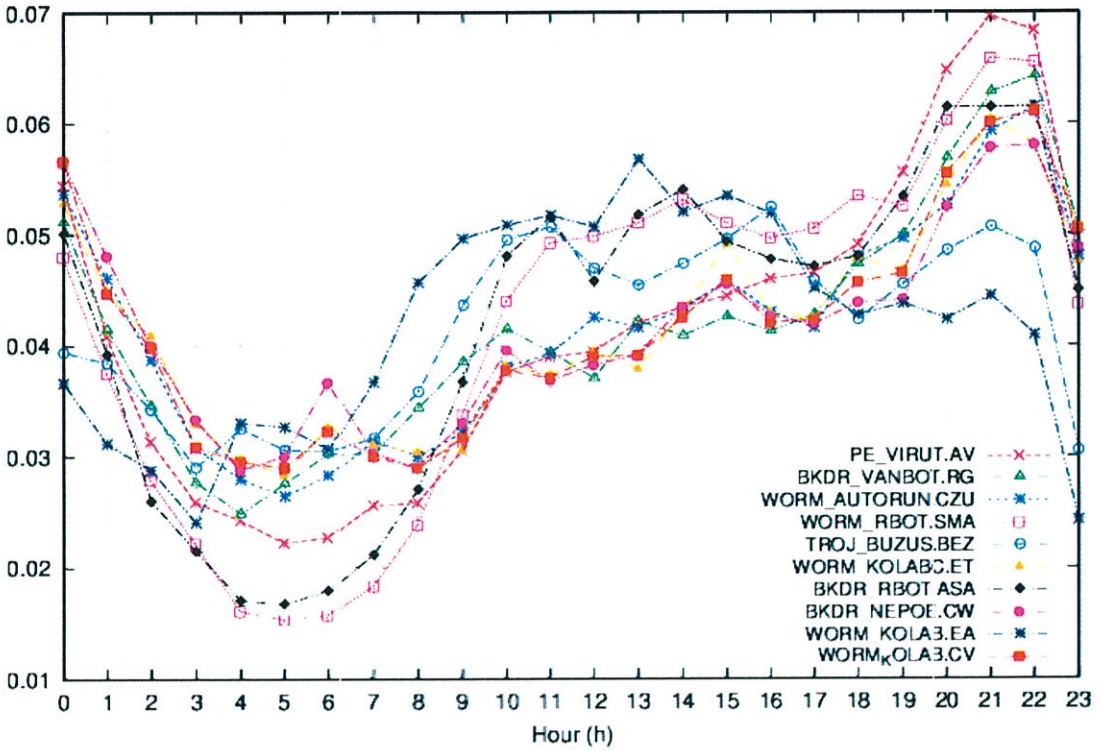
ค่าเฉลี่ยการดาวน์โหลด Top-10 มัลแวร์/บ็อทรายชั่วโมงของปี ค.ศ.2010-2011 ถูกแสดงเปรียบเทียบดังตารางที่ 4.2 ซึ่งจะพบว่า มัลแวร์ชื่อ PE_VIRUT.AV และ WORM_DOWNAD.AD มีค่าเฉลี่ยของการดาวน์โหลดมากที่สุดในปี ค.ศ.2010 และ 2011 ตามลำดับ

ตารางที่ 4.2 ค่าเฉลี่ยการดาวน์โหลด Top-10 มัลแวร์/บ็อท รายชั่วโมงของปี ค.ศ.2010-2011

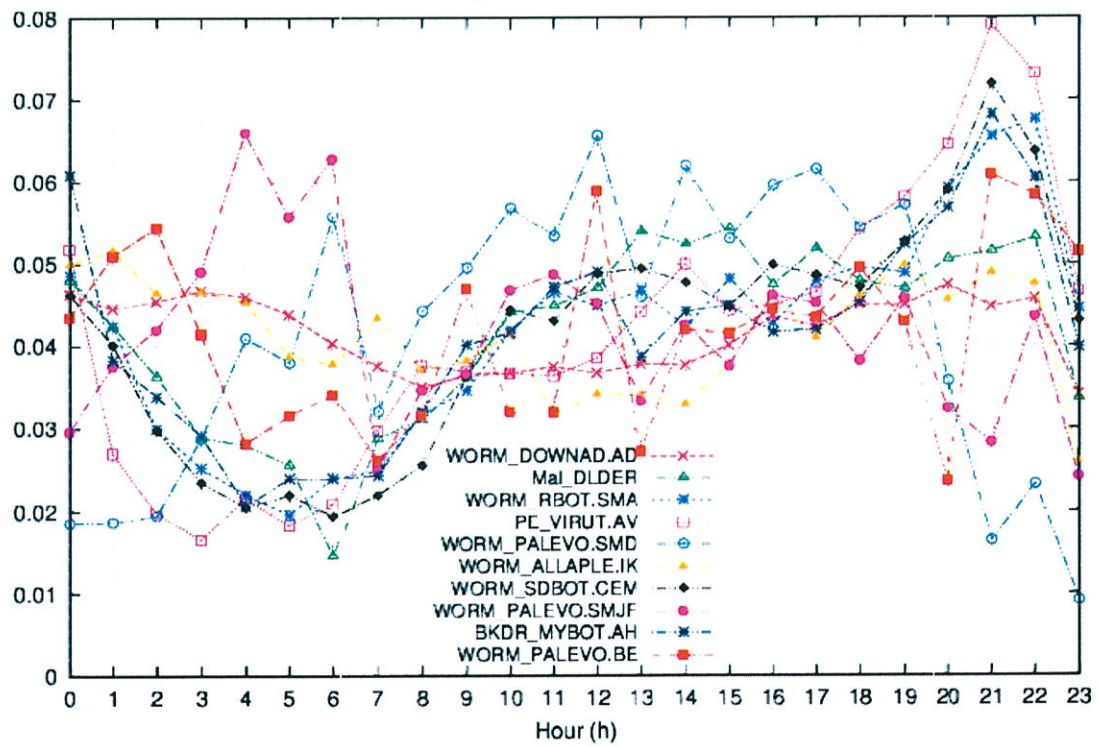
Top	2010		2011	
No	Malware	$\bar{l}_w^h$	Malware	$\bar{l}_w^h$
1	PE_VIRUT.AV	8,106	WORM_DOWNAD.AD	2,919
2	BKDR_VANBOT.RG	3,489	MAL_DLDER	754
3	WORM_AUTORUN.CZU	1,929	WORM_ RBOT.SMA	532
4	WORM_RBOT.SMA	1,507	PE_ VIRUT.AV	390
5	TROJ_BUZUS.BEZ	1,340	WORM_PALEVO.SMD	366
6	WORM_KOLABC.ET	1,331	WORM_ALLAPLE.IK	237
7	BKDR_RBOT.ASA	1,308	WORM_SDBOT.CEM	197
8	BKDR_NEPOE.CW	1,254	WORM_PALEVO.SMJF	130
9	WORM_KOLAB.EA	1,204	BKDR_MYBOT.AH	113
10	WORM_KOLAB.CV	1,191	WORM_PALEVO.BE	84

4.1.4 ค่านอร์มัลไลซ์ของการดาวน์โหลด Top-10 มัลแวร์/บ็อท รายชั่วโมงของปี ค.ศ.2010-2011

ค่านอร์มัลไลซ์ของการดาวน์โหลด Top-10 มัลแวร์/บ็อท รายชั่วโมงของปี ค.ศ.2010-2011 ถูกแสดงดังรูปที่ 4.3 และรูปที่ 4.4 ซึ่งแสดงให้เห็นว่ามัลแวร์/บ็อทจะถูกดาวน์โหลดมากในช่วงเวลากลางคืน (ตั้งแต่เวลา 19.00 น. – 23.00 น.) จนถึงเวลาเที่ยงคืน ถึงแม้ว่า Honeypots จะถูกเปิดใช้งานตลอดเวลาก็ตาม แต่มัลแวร์/บ็อทก็ถูกดาวน์โหลดค่อนข้างน้อยในช่วงเวลาหลังเที่ยงคืนถึงรุ่งเช้า



รูปที่ 4.3 ค่านอร์มัลไลซ์ของการดาวน์โหลด Top-10 มัลแวร์/บ็อทรายชั่วโมงของปี ค.ศ.2010



รูปที่ 4.4 ค่านอร์มัลไลซ์ของการดาวน์โหลด Top-10 มัลแวร์/บ็อทรายชั่วโมงของปี ค.ศ.2011

จากรูปที่ 4.3 และ 4.4 จะพบว่า รูปแบบของการดาวน์โหลดมัลแวร์/บ็อทในปี ค.ศ.2011 มีความคล้ายคลึงกับปี ค.ศ.2010 โดยมัลแวร์/บ็อทจะถูกดาวน์โหลดมากในช่วงเวลากลางคืน (ตั้งแต่เวลา 19.00 น. – 23.00 น.) จนถึงเวลาเที่ยงคืน แต่พฤติกรรมการดาวน์โหลดมัลแวร์/บ็อทในปี ค.ศ. 2011 ไม่ค่อยมีความสอดคล้องกันเหมือนปี ค.ศ.2010 ซึ่งมีความสอดคล้องกันมากกว่า ทั้งนี้ส่วนหนึ่งอาจมาจากปริมาณของล็อกข้อมูลในปี ค.ศ.2011 ที่นำมาวิเคราะห์มีปริมาณน้อยกว่า รวมถึงจำนวน Honeypots และช่วงเวลาที่น้อยกว่าปี ค.ศ.2010

4.1.5 จำนวนไอพี แอดเดรสของ Top-10 มัลแวร์ ที่มาจากต้นทางเดียวกันของปี ค.ศ.2010-2011

จากการวิเคราะห์พบว่า จำนวนไอพี แอดเดรสของ Top-10 มัลแวร์ ที่มาจากต้นทางเดียวกันในปี ค.ศ.2010 ตามตารางที่ 4.3 มีดังนี้

1) BKDR_VANBOT.RG, WORM_KOLABC.ET, BKDR_NEPOE.CW และ WORM_KOLAB.CV มาจากไอพี แอดเดรส 67.215.1.206 (ช่องสีเหลือง)

2) WORM_RBOT.SMA และ BKDR_RBOT.ASA มาจากไอพี แอดเดรส 60.249.10.8 และ 118.130.251.126 (ช่องสีแดง)

3) TROJ_BUZUS.BEZ และ WORM_KOLAB.EA มาจากไอพี แอดเดรส 91.207.7.116 และ 98.126.47.46 (ช่องสีฟ้า)

ตารางที่ 4.4 มีเพียงแค่ WORM_PALEVO.SMD และ WORM_PALEVO.SMJF ที่มาจากไอพี แอดเดรส 208.53.183.20 ในปี ค.ศ.2011

ตารางที่ 4.3 จำนวนไอพีแอดเดรสของ Top-10 มัลแวร์/บ็อท ที่มาจากต้นทางเดียวกันปี ค.ศ.2010

TOP	2	3	4	5	6	7	8	9	10
2					1		1		1
3									
4						2			
5								2	
6	1						1		1
7			2						
8	1				1				1
9				2					
10	1				1		1		

หมายเหตุ : 1.PE_VIRUT.AV 2.BKDR_VANBOT.RG 3.WORM_AUTORUN.CZU 4.WORM_RBOT.SMA 5.TROJ_BUZUS.BEZ 6.WORM_KOLABC.ET 7.BKDR_RBOT.ASA 8.BKDR_NEPOE.CW 9.WORM_KOLAB.EA 10.WORM_KOLAB.CV

ตารางที่ 4.4 จำนวนไอพี แอดเดรสของ Top-10 มัลแวร์/บ็อท ที่มาจากต้นทางเดียวกันปี ค.ศ.2011

TOP	2	3	4	5	6	7	8	9	10
1									
2									
3									
4									
5							1		
6									
7									
8				1					
9									

หมายเหตุ : 1.WORM_DOWNAD.AD 2.Mal_DLDER 3.WORM_RBOT.SMA 4.PE_VIRUT.AV 5.WORM_PALEVO.SMD 6.WORM_ALLAPLE.IK 7.WORM_SDBOT.CEM 8.WORM_PALEVO.SMJF 9.BKDR_MYBOT.AH 10.WORM_PALEVO.BE

4.1.6 Top-10 มัลแวร์/บ็อทที่มาจากไอพี แอดเดรสซับเน็ตเดียวกันของปี ค.ศ.2010-2011

จากล็อกข้อมูล CCC Datasets ของปี ค.ศ.2010-2011 ทำให้สามารถหา Top-10 มัลแวร์/บ็อท ที่มาจากไอพี แอดเดรสซับเน็ตเดียวกันได้ดังต่อไปนี้

Top-10 มัลแวร์/บ็อทที่มาจากไอพี แอดเดรสซับเน็ตเดียวกัน ปี ค.ศ.2010

1. PE_VIRUT.AV มาจาก ไอพี แอดเดรสซับเน็ตเดียวกัน ได้แก่

1.1) 122.135.180.217 และ 122.135.59.134

1.2) 118.109.21.235, 118.109.93.40 และ 118.109.56.137

1.3) 61.7.240.163

2. BKDR_VANBOT.RG มาจาก ไอพี แอดเดรสซับเน็ตเดียวกัน ได้แก่

2.1) 61.7.229.17

2.2) 121.9.236.151 และ 121.9.227.229

2.3) 67.215.1.206

3. WORM_AUTORUN.CZU มาจาก ไอพี แอดเดรสซับเน็ตเดียวกัน ได้แก่ 72.10.166.195

4. WORM_RBOT.SMA มาจาก ไอพี แอดเดรสซับเน็ตเดียวกัน ได้แก่

4.1) 118.232.18.45

4.2) 60.249.10.8 และ 60.249.204.192

4.3) 118.130.251.126

5. TROJ_BUZUS.BEZ มาจาก ไอพี แอดเดรสซับเน็ตเดียวกัน ได้แก่

5.1) 98.126.47.46

5.2) 91.207.7.116

6. WORM_KOLABC.ET มาจาก ไอพี แอดเดรสซับเน็ตเดียวกัน ได้แก่

6.1) 122.135.101.116 และ 122.135.42.237

6.2) 67.215.1.206

7. BKDR_RBOT.ASA มาจาก ไอพี แอดเดรสซับเน็ตเดียวกัน ได้แก่

7.1) 122.213.177.178 และ 122.213.230.203

7.2) 118.232.208.229

7.3) 118.130.251.126

7.4) 60.249.10.8

8. BKDR_NEPOE.CW มาจาก ไอพี แอดเดรสซับเน็ตเดียวกัน ได้แก่

8.1) 122.135.188.232, 122.135.131.230 และ 122.135.163.90

8.2) 67.215.1.206

9. WORM_KOLAB.EA มาจาก ไอพี แอดเดรสซับเน็ตเดียวกัน ได้แก่

9.1) 91.207.7.120 และ 91.207.7.116

9.2) 98.126.10.155 และ 98.126.47.46

10. **WORM_KOLAB.CV** มาจาก ไอพี แอดเดรสซับเน็ตเดียวกัน ได้แก่

10.1) 67.215.1.206

10.2) 72.10.169.26

ตารางที่ 4.5 บริษัทผู้ให้บริการอินเทอร์เน็ตของ Top-10 มัลแวร์/บ็อท ปี ค.ศ.2010

Country	ISP	IP Address	Malware Names	จำนวนการดาวน์โหลด
Canada	GloboTech Communications	67.215.X.X	BKDR_VANBOT.RG	55,068
			WORM_KOLABC.ET	24,514
			BKDR_NEPOE.CW	22,970
			WORM_KOLAB.CV	28,544
		72.10.X.X	WORM_AUTORUN.CZU	46,313
			WORM_KOLAB.CV	42
China	China Telecom Guangdong	121.9.X.X	BKDR_VANBOT.RG	647
Japan	NEC BIGLOBE	118.109.X.X	PE_VIRUT.AV	1,077
		122.135.X.X	PE_VIRUT.AV	692
			WORM_KOLABC.ET	611
			BKDR_NEPOE.CW	624
	UCOM	122.213.X.X	BKDR_RBOT.ASA	99
Korea	LG DACOM	118.130.X.X	WORM_RBOT.SMA	90
			BKDR_RBOT.ASA	90
Thailand	CAT Telecom public	61.7.X.X	PE_VIRUT.AV	908
			BKDR_VANBOT.RG	245
Taiwan	CHTD, Chunghwa Telecom	60.249.X.X	WORM_RBOT.SMA	133
			BKDR_RBOT.ASA	91
	TUNG HO MULTIMEDIA	118.232.X.X	WORM_RBOT.SMA	43
			BKDR_RBOT.ASA	63
Ukraine	PP Andrey Kiselev	91.207.X.X	TROJ_BUZUS.BEZ	10,550
			WORM_KOLAB.EA	19,107
United States	Krypt Technologies	98.126.X.X	TROJ_BUZUS.BEZ	7,564
			WORM_KOLAB.EA	9,800

Top-10 มัลแวร์/บ็อทที่มาจากไอพี แอดเดรสซับเน็ตเดียวกัน ปี ค.ศ.2011

1. **WORM_DOWNAD.AD** มาจาก ไอพี แอดเดรสซับเน็ตเดียวกัน ได้แก่

1.1) 111.255.74.79, 111.255.81.16

1.2) 122.118.68.88, 122.118.69.12

2. WORM_RBOT.SMA มาจาก ไอพี แอดเดรสซับเน็ตเดียวกัน ได้แก่

2.1) 60.249.10.8, 60.249.37.106 และ 60.249.204.192

2.2) 220.134.181.56

2.3) 125.100.167.47

3. PE_VIRUT.AV มาจาก ไอพี แอดเดรสซับเน็ตเดียวกัน ได้แก่

3.1) 121.102.41.126 และ 121.102.41.62

3.2) 211.135.79.6 และ 211.135.67.150

3.3) 120.75.27.34

3.4) 220.100.115.39, 220.100.114.46 และ 220.100.15.147

4. WORM_PALEVO.SMD มาจาก ไอพี แอดเดรสซับเน็ตเดียวกัน ได้แก่ 208.53.183.20

5. WORM_SDBOT.CEM มาจาก ไอพี แอดเดรสซับเน็ตเดียวกัน ได้แก่

5.1) 125.197.34.38, 125.197.107.94, 125.197.15.185 และ 125.197.105.202

5.2) 120.75.24.232.21

5.3) 58.80.235.57

6. WORM_PALEVO.SMJF มาจาก ไอพี แอดเดรสซับเน็ตเดียวกัน ได้แก่

6.1) 124.44.210.250, 124.44.202.250, 124.44.181.64 และ 124.44.181.200

6.2) 122.133.107.129

6.3) 124.45.160.240 และ 124.45.159.44

6.4) 208.53.183.20

7. BKDR_MYBOT.AH มาจาก ไอพี แอดเดรสซับเน็ตเดียวกัน ได้แก่

7.1) 58.80.212.28

7.2) 125.100.235.39

7.3) 220.134.182.9

8. **WORM_PALEVO.BE** มาจาก ไอพี แอดเดรสซับเน็ตเดียวกัน ได้แก่

8.1) 122.133.15.5

8.2) 211.135.69.8 และ 211.135.76.119

ตารางที่ 4.6 บริษัทผู้ให้บริการอินเทอร์เน็ตของ Top-10 มัลแวร์/บ็อท ปี ค.ศ.2011

Country	ISP	IP Address	Malware Names	จำนวนการดาวน์โหลด
Japan	UCOM	58.80.X.X	WORM_SDBOT.CEM	26
			BKDR_MYBOT.AH	12
	So-net Entertainment	125.100.X.X	WORM_RBOT.SMA	40
			BKDR_MYBOT.AH	16
	Internet Initiative Japan	120.75.X.X	PE_VIRUT.AV	88
			WORM_SDBOT.CEM	21
		121.102.X.X	PE_VIRUT.AV	186
	NEC BIGLOBE	220.100.X.X	PE_VIRUT.AV	370
		122.133.X.X	WORM_PALEVO.SMJF	33
			WORM_PALEVO.BE	67
	NTT-ME Corporation	125.197.X.X	WORM_SDBOT.CEM	79
		124.44.X.X	WORM_PALEVO.SMJF	228
	Kansai Multimedia Service	124.45.X.X	WORM_PALEVO.SMJF	81
		211.135.X.X	PE_VIRUT.AV	214
			WORM_PALEVO.BE	61
Taiwan	CHTD, Chunghwa Telecom	60.249.X.X	WORM_RBOT.SMA	87
		111.255.X.X	WORM_DOWNAD.AD	26
		220.134.X.X	WORM_RBOT.SMA	28
			BKDR_MYBOT.AH	26
	Chunghwa Telecom Data Communication Business Group	122.118.X.X	WORM_DOWNAD.AD	41
United States	FDCservers.net	208.53.X.X	WORM_PALEVO.SMD	8,784
			WORM_PALEVO.SMJF	1,787

นอกจากนี้ยังพบว่า มีมัลแวร์ชนิดเดียวกันที่แพร่กระจายไปยังเครื่องคอมพิวเตอร์ของเหยื่อในประเทศต่างๆ ของปี ค.ศ.2010 ดังตารางที่ 4.7 และของปี ค.ศ.2011 ดังตารางที่ 4.8 ตามลำดับ

ตารางที่ 4.7 มัลแวร์ชนิดเดียวกันที่แพร่กระจายไปยังประเทศต่างๆ ของปี ค.ศ.2010

NO.	Malware Names	IP Address	ISP	Country	จำนวนการดาวน์โหลด
1	BKDR_VANBOT.RG	67.215.X.X	GloboTechCommunications	Canada	55,068
		121.9.X.X	China Telecom Guangdong	China	647
		61.7.X.X	CAT Telecom public	Thailand	245
					55,960
2	WORM_KOLAB.EA	91.207.X.X	PP Andrey Kiselev	Ukraine	19,107
		98.126.X.X	Krypt Technologies	United States	9,800
					28,907
3	WORM_KOLABC.ET	67.215.X.X	GloboTechCommunications	Canada	24,514
		122.135.X.X	NEC BIGLOBE	Japan	611
					25,125
4	BKDR_NEPOE.CW	67.215.X.X	GloboTechCommunications	Canada	22,970
		122.135.X.X	NEC BIGLOBE	Japan	624
					23,594
5	TROJ_BUZUS.BEZ	91.207.X.X	PP Andrey Kiselev	Ukraine	10,550
		98.126.X.X	Krypt Technologies	United States	7,564
					18,114
6	PE_VIRUT.AV	118.109.X.X	NEC BIGLOBE	Japan	1,077
		122.135.X.X	NEC BIGLOBE	Japan	692
		61.7.X.X	CAT Telecom public	Thailand	908
					2,677
7	BKDR_RBOT.ASA	122.213.X.X	UCOM	Japan	99
		118.130.X.X	LG DACOM	Korea	90
		60.249.X.X	CHTD, Chunghwa Telecom	Taiwan	91
		118.232.X.X	TUNG HO MULTIMEDIA	Taiwan	63
					343
8	WORM_RBOT.SMA	118.130.X.X	LG DACOM	Korea	90
		60.249.X.X	CHTD, Chunghwa Telecom	Taiwan	133
		118.232.X.X	TUNG HO MULTIMEDIA	Taiwan	43
					266

ตารางที่ 4.8 มัลแวร์ชนิดเดียวกันที่แพร่กระจายไปยังประเทศต่างๆ ของปี ค.ศ.2011

NO.	Malware Names	IP Address	ISP	Country	จำนวนการดาวน์โหลด
1	WORM_RBOT.SMA	125.100.X.X	So-net Entertainment	Japan	40
		60.249.X.X	CHTD, Chunghwa Telecom	Taiwan	87
		220.134.X.X	CHTD, Chunghwa Telecom	Taiwan	28
					155
2	BKDR_MYBOT.AH	58.80.X.X	UCOM	Japan	12
		125.100.X.X	So-net Entertainment	Japan	16
		220.134.X.X	CHTD, Chunghwa Telecom	Taiwan	26
					54

จากตารางที่ 4.7 พบว่า มีมัลแวร์ชนิดเดียวกันที่แพร่กระจายไปยังเครื่องคอมพิวเตอร์ของเหยื่อในประเทศต่างๆ ของปี ค.ศ.2010 จำนวน 8 ชนิด ได้แก่ BKDR_VANBOT.RG, WORM_KOLAB.EA, WORM_KOLABC.ET, BKDR_NEPOE.CW, TROJ_BUZUS.BEZ, PE_VIRUT.AV, BKDR_RBOT.ASA และ WORM_RBOT.SMA ซึ่งมีการดาวน์โหลดมัลแวร์ WORM_RBOT.SMA เยอะที่สุดถึง 55,960 ครั้ง

ส่วนตารางที่ 4.8 มีมัลแวร์ชนิดเดียวกันที่แพร่กระจายไปยังเครื่องคอมพิวเตอร์ของเหยื่อในประเทศต่างๆ ของปี ค.ศ.2011 เพียงแค่ 2 ชนิดเท่านั้น คือ BKDR_MYBOT.AH และ WORM_RBOT.SMA ซึ่งมีการดาวน์โหลดมัลแวร์ดังกล่าว 155 ครั้ง และ 54 ครั้ง ตามลำดับ

บทที่ 5
สรุปผลการวิจัยและข้อเสนอแนะ

5.1 สรุปผลการวิจัย

วิทยานิพนธ์ฉบับนี้ได้ทำการวิเคราะห์พฤติกรรมการดาวน์โหลดของ Top-10 มัลแวร์/บ็อท โดยใช้ล็อกข้อมูล CCC ของ ปี ค.ศ.2010 และ 2011 โดยแสดงผลในรูปของกราฟการดาวน์โหลดแบบรายชั่วโมง และรายวัน ซึ่งกราฟในปี ค.ศ.2010 จะมีพฤติกรรมการดาวน์โหลดที่มีความสัมพันธ์กัน และการดาวน์โหลดส่วนใหญ่จะเป็นช่วงต้นปีงบประมาณของประเทศญี่ปุ่น ซึ่งมีความแตกต่างจากกราฟของปี ค.ศ.2011 ที่ไม่มีความสัมพันธ์กันเท่าไรนัก และพบว่ามัลแวร์/บ็อทจะถูกดาวน์โหลดมากในช่วงเวลากลางคืน (ตั้งแต่เวลา 19.00 น. – 23.00 น.) จนถึงเวลาเที่ยงคืน

ไอพี แอดเดรสของ Top-10 มัลแวร์/บ็อท ที่มาจากไอพี แอดเดรสซับเน็ตเดียวกันในปี ค.ศ. 2010 มีจำนวน 12 ไอพีแอดเดรส ได้แก่ 67.215.X.X, 72.10.X.X, 121.9.X.X, 118.109.X.X, 122.135.X.X, 122.213.X.X, 118.130.X.X, 61.7.X.X, 60.249.X.X, 118.232.X.X, 91.207.X.X และ 98.126.X.X ส่วนไอพี แอดเดรสของ Top-10 มัลแวร์/บ็อท ที่มาจากไอพี แอดเดรสซับเน็ตเดียวกันในปี ค.ศ.2011 มีจำนวน 15 ไอพีแอดเดรส ได้แก่ 58.80.X.X, 125.100.X.X, 120.75.X.X, 121.102.X.X, 220.100.X.X, 122.133.X.X, 125.197.X.X, 124.44.X.X, 124.45.X.X, 211.135.X.X, 60.249.X.X, 111.255.X.X, 220.134.X.X, 122.118.X.X และ 208.53.X.X อีกทั้งจำนวนไอพี แอดเดรสของ Top-10 มัลแวร์ที่มาจากต้นทางเดียวกันในปี ค.ศ.2010 มีจำนวน 5 ไอพี แอดเดรส ต่างจากปี ค.ศ. 2011 ที่มีเพียง 1 ไอพี แอดเดรส

ส่วนมัลแวร์ชนิดเดียวกันที่แพร่กระจายไปยังเครื่องคอมพิวเตอร์ของเหยื่อในประเทศต่างๆ ของปี ค.ศ.2010 จำนวน 8 ชนิด ได้แก่ BKDR_VANBOT.RG, WORM_KOLAB.EA, WORM_KOLABC.ET, BKDR_NEPOE.CW, TROJ_BUZUS.BEZ, PE_VIRUT.AV, BKDR_RBOT.ASA และ WORM_RBOT.SMA ซึ่งมีการดาวน์โหลดมัลแวร์ WORM_RBOT.SMA เยอะที่สุดถึง 55,960 ครั้ง และมัลแวร์ชนิดเดียวกันที่แพร่กระจายไปยังเครื่องคอมพิวเตอร์ของเหยื่อในประเทศต่างๆ ของปี ค.ศ.2011 เพียงแค่ 2 ชนิดเท่านั้น คือ BKDR_MYBOT.AH และ WORM_RBOT.SMA ซึ่งมีการดาวน์โหลดมัลแวร์ดังกล่าว 155 ครั้ง และ 54 ครั้ง ตามลำดับ

5.2 ข้อเสนอแนะ

จากการวิจัยในวิทยานิพนธ์ฉบับนี้จะพบว่าล็อกข้อมูล CCC ของปี ค.ศ.2011 (ใช้ล็อกข้อมูล CCC 9 เดือน) มีปริมาณน้อยกว่าปี ค.ศ.2010 (ใช้ล็อกข้อมูล CCC 12 เดือน) ซึ่งทำให้กราฟที่ออกมาไม่มีความสัมพันธ์กันเท่าไรนัก จึงควรใช้ล็อกข้อมูลในช่วงเวลา 12 เดือนเท่ากัน ซึ่งอาจทำให้งานวิจัยออกมาถูกต้อง และสมบูรณ์มากยิ่งขึ้น

ในช่วงเวลาที่มีมัลแวร์/บ็อทกระจายตัวมากที่สุด คือช่วงเวลา 19.00 น. เป็นต้นไป จนถึงเวลาเที่ยงคืนนั้น ผู้ใช้พึงระมัดระวังในการเข้าใช้งานอินเทอร์เน็ต อีเมล์ หรือโซเชียลมีเดีย (Social Media)

ต่างๆ โดยทำการอัพเดตหรือแพตช์เพื่ออุดช่องโหว่ของวินโดวส์อย่างสม่ำเสมอ รวมถึงเปิดการทำงานไฟร์วอลล์ของวินโดวส์ หรือซอฟต์แวร์ไฟร์วอลล์ที่ผู้ใช้ติดตั้งเพิ่มเติมภายหลัง และไม่ควรเข้าหน้าเว็ปไซต์ หรือคลิกลิ้งค์ หรือเปิดอ่านเมล์ หรือดาวน์โหลดไฟล์ที่ไม่รู้จักอย่างเด็ดขาด เพราะอาจจะทำให้ผู้ใช้ติดมัลแวร์/บ็อทได้โดยรู้เท่าไม่ถึงการณ์

เอกสารอ้างอิง

[1] M.Hatada, Y.Nakatsuru, M.Akiyama and S.Miwa, **"Datasets for anti malware research,"** IPSJ anti Malware engineering Workshop 2010 (MWS2010), 2010.

[2] N.R.Rosyid , M.Ohrui, H.Kikuchi, P.Sooraksa and M.Terada, **"A discovery of sequential attack patterns of malware in bontents,"** IEEE International Conference on System Man and Cybermetics (SMC), vol. Vol.2010-CSEC-48, No.37, pp. pp.2564-2570, October 2010.

[3] J.Song, J.Shimamura, M.Eto, D.Inoue and K.Nakao **"Correlation analysis between spamming botnets and malware infected hosts,"** in IEEE/IPSJ 11th International Symposium on Applications and the Internet (SAINT), July 2011, pp. pp.372-375.

[4] K.Sisaat, H.Kikuchi, S.Matsuo, M.Terada, M.Fujiwara and S.Kittitornkun, **"Time zone correlation analysis of malware/bot downloads,"** To be published in IEICE Transactions on Communications, vol. Vol.E96-B, No.07, 2013.

ภาคผนวก

ภาคผนวก ก.
ผลงานวิจัยที่ได้รับการตีพิมพ์เผยแพร่

[1] วัชรวิชญ์ สุวรรณชัยศักดิ์ และคณะ. 2557. “ผลวิเคราะห์ข้อมูลการดาวน์โหลดมัลแวร์/บ็อทในญี่ปุ่น” หน้า 242-249. ใน **การประชุมวิชาการ ครั้งที่** 52 **มหาวิทยาลัยเกษตรศาสตร์ เล่มที่** 5 **สาขาสถาปัตยกรรมศาสตร์และวิศวกรรมศาสตร์.** กรุงเทพฯ : มหาวิทยาลัยเกษตรศาสตร์

ภาคผนวก ข.
คุณสมบัติของ Top-10 มัลแวร์ ปี ค.ศ.2010

Top	Malware Names	Threats	Infection Channel	Aliases
1	PE_VIRUT.AV	ทำการเขียนทับรหัส (Code) ที่ตรวจพบไปยังไฟล์เป้าหมาย แล้วเพิ่มโครงสร้าง virus body ไปยังไฟล์ดังกล่าว สุดท้ายโค้ดจะถูกบันทึกใน virus body ซึ่งรูปแบบไฟล์ที่ติดเชื้อส่วนใหญ่จะเป็น .EXE และ .SCR	ติดเชื้อโดยการดาวน์โหลดจากอินเทอร์เน็ต หรือติดเชื้อจากมัลแวร์ชนิดอื่นๆ	W32/Virut.gen.a (McAfee), Virus.Win32.Virut.a (v) (Sunbelt) Win32/Virut.AV virus (Eset)
2	BKDR_VANBOT.RG	เป็นชนิด backdoor จะทำการคัดลอกตัวมันเองไปยังโฟลเดอร์ (folder) %System%\winamp.exe ซึ่ง %System% ก็คือโฟลเดอร์ Windows system และจะทำการลบไฟล์ %System%\winamp.exe และ %System Root%\vreov.bat	ติดเชื้อโดยการดาวน์โหลดไฟล์ที่ไม่รู้จักจากเว็บไซต์ที่มีมัลแวร์หรือติดเชื้อจากมัลแวร์ชนิดอื่นๆ	VirTool:Win32/DelfInject.gen!BD (Microsoft) W32/Hamweq.worm.h (McAfee), W32.IRCBot (Symantec), Backdoor.Win32.VanBot.bdt (Kaspersky), Backdoor.Win32.EggDrop.bmg (v) (Sunbelt)
3	WORM_AUTORUN.CZU	เป็นหนอนอินเทอร์เน็ต (worm) กระจายตัวเองไปยังเครือข่ายต่างๆ ซึ่งหนอนอินเทอร์เน็ตไม่ใช่ infect file แต่ตัวมันจะมี payloads ที่สามารถผ่านระบบความปลอดภัยทางคอมพิวเตอร์ได้และขโมยข้อมูลสารสนเทศในที่สุด	ติดมัลแวร์ผ่านทางอีเมล์ (e-mail), IRC, network share, instant messenger (IM) และ peer-to-peer (P2P) networks	P2P-Worm.Win32.Palevo.brx (Kaspersky), W32.SillyFDC (Symantec), Worm/Agent.W.45 (Avira)
4	WORM_RBOT.SMA	เป็นหนอนอินเทอร์เน็ต (worm) กระจายตัวเองไปยังเครือข่ายต่างๆ ซึ่งหนอนอินเทอร์เน็ตไม่ใช่ infect file แต่ตัวมันจะมี payloads ที่สามารถผ่านระบบความปลอดภัยทางคอมพิวเตอร์ได้และขโมยข้อมูลสารสนเทศในที่สุด	ติดมัลแวร์ผ่านทางอีเมล์ (e-mail), IRC, network share, instant messenger (IM) และ peer-to-peer (P2P) networks	-

Top	Malware Names	Threats	Infection Channel	Aliases
5	TROJ_BUZUS.BEZ	เป็นม้าโทรจัน (trojan horse) จะทำการคัดลอกตัวมันเองไปยังโฟลเดอร์ (folder) %System Root% \WIN\DOWS\LAX.exe ซึ่ง %System Root% ก็คือโฟลเดอร์ root และจะทำการสร้างโฟลเดอร์ %System Root%\WIN และ %System Root% \WIN\DOWS อีกทั้งจะทำการลบไฟล์ %System Root% \WIN\DOWS\LAX.ex	ติดเชื้อโดยการดาวน์โหลดไฟล์ที่ไม่รู้จักจากเว็บไซต์ที่มีมัลแวร์หรือติดเชื้อจากมัลแวร์ชนิดอื่นๆ	VirTool:Win32/Vbinder.gen!GL (Microsoft), Generic.dx!dqv (McAfee), Trojan Horse (Symantec), Trojan.Win32.VB.umo (Kaspersky), Virtool.Win32.Vbinject.1 (v) (Sunbelt), Trojan horse VBCrypt.CZL (AVG)
6	WORM_KOLABC.ET	เป็นหนอนอินเทอร์เน็ต (worm) จะทำการคัดลอกตัวมันเองไปยังโฟลเดอร์ (folder) %Windows% \Fonts\unwise_.exe ซึ่ง %Windows% ก็คือโฟลเดอร์ Windows	ติดเชื้อโดยการดาวน์โหลดไฟล์ที่ไม่รู้จักจากเว็บไซต์ที่มีมัลแวร์หรือติดเชื้อจากมัลแวร์ชนิดอื่นๆ	Exploit:Win32/MS08067.gen!A (Microsoft), W32/Kolab (McAfee), W32.Spybot.Worm (Symantec), Net-Worm.Win32.Kolabc.hki (Kaspersky), BehavesLike.Win32.Malware.eah (mx-v) (Sunbelt), Win32.Worm.Kolabc.V (FSecure)
7	BKDR_RBOT.ASA	เป็นชนิด backdoor คอยแพร่กระจายไฟล์ %System%\{random}.exe ให้เครื่องอื่นๆ ติดเชื้อ ซึ่ง %System% ก็คือโฟลเดอร์ Windows system	ติดเชื้อโดยการดาวน์โหลดจากอินเทอร์เน็ต หรือติดเชื้อจากมัลแวร์ชนิดอื่นๆ	Backdoor.Win32.Rbot.rax (Kaspersky), W32/Sdbot.worm.gen.x (McAfee), W32.Spybot.Worm (Symantec), W32/Trojan5.DCW (exact) (F-Prot)
8	BKDR_NEPOE.CW	เป็นชนิด backdoor ทำการแก้ไขค่าของระบบให้ทำงานโดยอัตโนมัติ และคอยเปิดช่องทางให้ผู้ไม่หวังดีเข้ามาควบคุมระบบ	ติดเชื้อโดยการดาวน์โหลดจากอินเทอร์เน็ต หรือติดเชื้อจากมัลแวร์ชนิดอื่นๆ	Backdoor.IRCBot!sd5 (PCTools), W32.IRCBot (Symantec), Generic.dx (McAfee)

Top	Malware Names	Threats	Infection Channel	Aliases
9	WORM_KOLAB.EA	เป็นหนอนอินเทอร์เน็ต (worm) จะทำการคัดลอกตัวมันเองไปยังโฟลเดอร์ (folder) %System Root%\RECYCLER\S-1-5-21-0243556031-888888379-781863308-1455\fjidg.exe ซึ่ง %System Root% ก็คือโฟลเดอร์ root และจะทำการสร้างโฟลเดอร์ %System Root%\RECYCLER และ %System Root%\RECYCLER\S-1-5-21-0243556031-888888379-781863308-1455 อีกทั้งจะทำการลบไฟล์ %System Root%\RECYCLER\S-1-5-21-0243556031-888888379-781863308-1455\fjidg.exe	ติดเชื้อโดยการดาวน์โหลดไฟล์ที่ไม่รู้จักจากเว็บไซต์ที่มีมัลแวร์หรือติดเชื้อจากมัลแวร์ชนิดอื่นๆ	Trojan:Win32/Lethic.H (Microsoft), Generic.ge (McAfee), Trojan.Gen (Symantec), Trojan.Win32.Buzus.ctfx (Kaspersky), Trojan.Win32.Buzus.bzaz (v) (Sunbelt), Worm:W32/Palevo.gen!J (FSecure)
10	WORM_KOLAB.CV	เป็นหนอนอินเทอร์เน็ต (worm) จะทำการคัดลอกตัวมันเองไปยังโฟลเดอร์ (folder) %System Root%\RECYCLER\S-1-5-21-1163389800-3766403717-517084011-2148\hdav.exe ซึ่ง %System Root% ก็คือโฟลเดอร์ root และจะทำการสร้างโฟลเดอร์ %System Root%\RECYCLER และ %System Root%\RECYCLER\S-1-5-21-1163389800-3766403717-517084011-2148 อีกทั้งจะแพร่กระจายไฟล์ %System Root%\RECYCLER\S-1-5-21-1163389800-3766403717-517084011-2148\Desktop.ini	ติดเชื้อโดยการดาวน์โหลดไฟล์ที่ไม่รู้จักจากเว็บไซต์ที่มีมัลแวร์หรือติดเชื้อจากมัลแวร์ชนิดอื่นๆ	VirTool:Win32/DelfInject.gen!BD (Microsoft), BackDoor-DOQ.gen.z (McAfee), W32.Spybot.Worm (Symantec), Net-Worm.Win32.Kolab.ffo (Kaspersky), NetWorm.Win32.Kolab.ffo (v) (Sunbelt) Trojan horse BackDoor.Generic12.ASZO (AVG)

ภาคผนวก ค.
คุณสมบัติของ Top-10 มัลแวร์ ปี ค.ศ.2011

Top	Malware Names	Threats	Infection Channel	Aliases
1	WORM_DOWNAD.AD	เป็นหนอนอินเทอร์เน็ต (worm) จะคัดลอกตัวมันเองไปใน physical และ removable drives, ส่งรหัส (exploit code) สุ่มไปยัง internet addresses, สร้างกลุ่มของ URLs ที่ประกอบด้วย 250 เว็บไซต์ต่อวันบนพื้นฐานเวลา UTC time, เข้าไปเปลี่ยนแปลงรีจีสทรี (registry) เพื่อหยุดการทำงานของระบบ และเปลี่ยนรีจีสทรีเพื่อซ่อน Hidden files และป้องกันผู้ใช้งานไม่ให้สามารถเข้าถึงเว็บไซต์ที่ป้องกันไวรัสได้ อีกทั้งยังปล่อยไฟล์ AUTORUN.INF เพื่อให้จัดการทำสำเนากับสิ่งที่มันปล่อยออกมาเมื่อมีผู้ใช้งานมาใช้ระบบนั้น	ติดเชื้อผ่านทาง removable drives, ช่องโหว่ของโปรแกรม และการใช้งานเครือข่ายร่วมกัน (network shares)	Win32.HLLW.Shadow.1 (Dr.Web), Win32.Worm.Downadup.H (BitDefender), Embedded.Net-Worm.Win32.Kido.ij (VirusBlokAda), TR/Dropper.Gen (Avira), Net-Worm.Win32.Kido.ih (Kaspersky), BEAV-New MS06-040 (McAfee), Worm:Win32/Conficker.C (Microsoft)
2	MAL_DLDER	เป็นประเภทม้าโทรจันและ keylogger ซึ่งสามารถขโมยข้อมูล เช่น รหัสบัญชี รหัสบัตรเครดิต และข้อมูลทางบัญชีต่างๆ เป็นต้น	ติดเชื้อโดยการดาวน์โหลดไฟล์ที่ไม่รู้จักจากเว็บไซต์ที่มีมัลแวร์ หรือติดเชื้อจากมัลแวร์ชนิดอื่นๆ	Downloader (Symantec), Trojan-Downloader.Win32.Small.gen (Kaspersky), TR/Downloader.Gen (Avira), W32/Heuristic-217!Eldorado (not disinfectable)(F-Prot), Downloader-FI.gen !! (McAfee)
3	WORM_RBOT.SMA	เป็นหนอนอินเทอร์เน็ต (worm) กระจายตัวเองไปยังเครือข่ายต่างๆ ซึ่งหนอนอินเทอร์เน็ตไม่ใช่ infect file แต่ตัวมันจะมี payloads ที่สามารถผ่านระบบความปลอดภัยทางคอมพิวเตอร์ได้และขโมยข้อมูลสารสนเทศในที่สุด	ติดมัลแวร์ผ่านทางอีเมล์ (e-mail), IRC, network share, instant messenger (IM) และ peer-to-peer (P2P) networks	-

Top	Malware Names	Threats	Infection Channel	Aliases
4	PE_VIRUT.AV	ทำการเขียนทับรหัส (Code) ที่ตรวจพบไปยังไฟล์เป้าหมาย แล้วเพิ่มโครงสร้าง virus body ไปยังไฟล์ดังกล่าว สุดท้ายโค้ดจะถูกบันทึกใน virus body ซึ่งรูปแบบไฟล์ที่ติดเชื้อส่วนใหญ่จะเป็น .EXE และ .SCR	ติดเชื้อโดยการดาวน์โหลดจากอินเทอร์เน็ต หรือติดเชื้อจากมัลแวร์ชนิดอื่นๆ	W32/Virut.gen.a (McAfee), Virus.Win32.Virut.a (v) (Sunbelt) Win32/Virut.AV virus (Eset)
5	WORM_PALEVO.SMD	เป็นหนอนอินเทอร์เน็ต (worm) จะทำการคัดลอกตัวมันเองไปยังโฟลเดอร์ (folder) %System Root%\RECYCLER\S-1-5-21-0243936033-3052116371-381863308-1811\vsbntlo.exe ซึ่ง %System Root% ก็คือโฟลเดอร์ root และจะทำการสร้างโฟลเดอร์ %System Root%\RECYCLER และ %System Root%\RECYCLER\S-1-5-21-0243936033-3052116371-381863308-1811 อีกทั้งจะทำการลบไฟล์ %System Root%\RECYCLER\S-1-5-21-0243936033-3052116371-381863308-1811\vsbntlo.exe	ติดเชื้อโดยการดาวน์โหลดไฟล์ที่ไม่รู้จักจากเว็บไซต์ที่มีมัลแวร์หรือติดเชื้อจากมัลแวร์ชนิดอื่นๆ	VirTool:Win32/DelfInject.gen!BH (Microsoft), BackDoor-EOC (McAfee), W32.Pilleuz!gen2, Packed.Generic.291 (Symantec), P2P-Worm.Win32.Palevo.rmm (Kaspersky), Virtool.Win32.DelfInject.gen.be (v) (Sunbelt), Trojan horse BackDoor.Generic12.BYLU (AVG)
6	WORM_ALLAPLE.IK	เป็นหนอนอินเทอร์เน็ต (worm) จะทำการสร้างและเพิ่มความเสียหายโดยวิธีการ DDOS attack ไปยังเว็บไซต์ที่ต้องการ ซึ่งมัลแวร์ชนิดนี้สามารถกระจายเพิ่มขึ้นผ่านทางช่องโหว่ของโปรแกรมและสำเนาตัวมันเองผ่านทางเครือข่ายที่ใช้งานร่วมกัน (network shares)	ติดเชื้อผ่านทางช่องโหว่ของโปรแกรม	W32.Rahack.W (Symantec), W32/RAHack (McAfee), WORM_ALLAPLE.IK (Trend Micro), W32/Allaple-F (Sophos), Net-Worm.Win32.Allaple (Ikarus)
7	WORM_SDBOT.CEM	เป็นหนอนอินเทอร์เน็ต (worm) จะทำการดักจับรหัสผ่าน (password) จากข้อมูลบนเครือข่าย, บันทึกข้อมูการใช้งานของผู้ใช้เมื่อมีการกดแป้นพิมพ์, ขโมย CD keys/serial number ของโปรแกรม, ทะลุผ่าน Windows firewall และโจมตีช่องโหว่ของโปรแกรม	แพร่กระจายผ่านทาง removable drives, เครือข่าย peer-to-peer, การใช้งานเครือข่ายร่วมกัน (nwtwork shares), ช่องโหว่ของโปรแกรม, IRC และดาวน์โหลดผ่านทางอินเทอร์เน็ต	Backdoor.Win32.Rbot.bqj (Kaspersky Lab), Backdoor:Win32/Rbot (Microsoft), W32.IRCBot(Symantec), W32/Sdbot.worm.gen.bs (McAfee), Win32/IRCBot.worm.variant (AhnLab), Worm.Rbot.VJV (PC Tools)

Top	Malware Names	Threats	Infection Channel	Aliases
8	WORM_PALEVO.SMJF	เป็นหนอนอินเทอร์เน็ต (worm) ทำให้การใช้งานอินเทอร์เน็ตช้าลง, ระบบปิดและเปิดเอง, โฆษณาเกิดขึ้นเต็มหน้าจอ และเกิดการปรับเปลี่ยนหน้าจอหลักของโฮมเพจ (home page) เอง	ติดเชื้อโดยการดาวน์โหลดไฟล์ที่ไม่รู้จักจากเว็ปไซต์ที่มีมัลแวร์หรือติดเชื้อจากมัลแวร์ชนิดอื่นๆ	TrojanProxy:Win32/Ranky.gen!B (Microsoft), Generic.ge (McAfee), Trojan.Gen (Symantec), Trojan.Win32.Buzus.ctfx (Kaspersky), Trojan.Win32.Buzus.bzaz (v) (Sunbelt), Worm:W32/Palevo.gen!J (FSecure)
9	BKDR_MYBOT.AH	เป็นชนิด backdoor ทำการแก้ไขค่าของระบบให้ทำงานโดยอัตโนมัติ และคอยเปิดช่องทางให้ผู้ไม่หวังดีเข้ามาควบคุมระบบ	ติดเชื้อโดยการดาวน์โหลดจากอินเทอร์เน็ต หรือติดเชื้อจากมัลแวร์ชนิดอื่นๆ	Backdoor.Win32.Rbot.bqj (Kaspersky), W32.Spybot.Worm (Symantec), Worm/Rbot.147456.27 (Avira), Mal/Generic-A (Sophos)
10	WORM_PALEVO.BE	เป็นหนอนอินเทอร์เน็ต (worm) กระจายตัวเองไปยังเครือข่ายต่างๆ ซึ่งหนอนอินเทอร์เน็ตไม่ใช่ infect file แต่ตัวมันจะมี payloads ที่สามารถผ่านระบบความปลอดภัยทางคอมพิวเตอร์ได้และขโมยข้อมูลสารสนเทศในที่สุด	ติดมัลแวร์ผ่านทางอีเมล์ (e-mail), IRC, network share, instant messenger (IM) และ peer-to-peer (P2P) networks.	VirTool:Win32/DelfInject.J (Microsoft), W32/IRCbot.gen.aj (McAfee), P2P-Worm.Win32.Palevo.nxs (Kaspersky), Trojan.Win32.Buzus.bzaz (v) (Sunbelt), Trojan horse Injector.JP (AVG)

ประวัติผู้เขียน

ชื่อ-นามสกุล	นายวัชรวิชญ์ สุวรรณชัยศักดิ์
วัน เดือน ปีเกิด	17 มีนาคม 2525 ที่นนทบุรี
ที่อยู่	299/511 หมู่บ้านมัณฑนา เลค วัชรพล ถ.สุขาภิบาล 5 แขวงสายไหม เขตสายไหม กรุงเทพฯ 10200
ประวัติการศึกษา	2547 วิทยาศาสตรบัณฑิต สาขาเทคโนโลยีคอมพิวเตอร์ สถาบันเทคโนโลยีราชมงคลธัญบุรี
ความชำนาญเฉพาะด้าน	ระบบคอมพิวเตอร์และเครือข่าย
ประสบการณ์การทำงาน	
พ.ศ.2547	ตำแหน่งโปรแกรมเมอร์ บริษัท คอมพิวเตอร์ไซน์ จำกัด
ปัจจุบัน	ตำแหน่งผู้ตรวจสอบ บริษัท ท่าอากาศยานไทย จำกัด (มหาชน)